

08-28-02

0360  
18\$  
#3

# ReedSmith

Carl H. Pierce • 215 241 7970 • cpierce@reedsmith.com

August 27, 2002

Commissioner of Patents and Trademarks  
Washington, D.C. 20231



RE: U.S. Patent Application Serial No.: 10/015,077 ✓  
Applicant: Turner et al.  
For: SYSTEM AND METHOD FOR USING AN INSTANT  
MESSAGING ENVIRONMENT TO ESTABLISH A HOSTED  
APPLICATION SHARING SESSION  
Attorney Docket No.: 01-40169-US (882397.20001)

Dear Sir:

Enclosed for filing in connection with the above-referenced patent application is the following document:

1. Petition to Withdraw Notice of Omitted Items in a Non-Provisional Application Under 37 CFR 1.181 (with Exhibits A through F); and
2. Check in the amount of \$130.00.

Kindly acknowledge receipt of this document by returning the enclosed self-addressed, stamped post card to me.

The Commissioner is hereby authorized to charge any additional fees required in connection with this filing to Account No. 18-0586.

Sincerely yours,

Carl H. Pierce

RECEIVED

SEP 24 2002

OFFICE OF PETITIONS

Enclosure

\* \* \* \* \*

**EXPRESS MAIL CERTIFICATE (37 CFR 1.10)**

Express Mail Label No.

EL16682122545

Date of Deposit

Aug 27, 2002

I hereby certify that this paper, and the papers and/or fees referred to herein as transmitted, submitted or enclosed, are being deposited with the U.S. Postal Service "Express Mail Post Office to Addressee" service under 37 CFR §1.10 on the date indicated above and is addressed to the Commissioner of Patents and Trademarks, Washington, D.C. 20231.

Name:

JUDITHA ZWEIG

Signature:

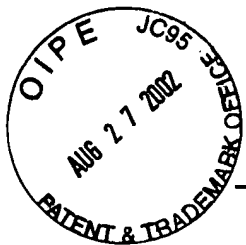
2500 One Liberty Place  
1650 Market Street  
Philadelphia, PA 19103-7301  
215.851.8100  
Fax 215.851.1420

Delaware  
New Jersey  
New York  
Pennsylvania  
Virginia  
Washington, DC

reedsmith.com

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Application of Turner et al. : Attorney Docket No.:  
Serial No.: 10/015,077 : 01-40169-US  
Conf. No.: 9530 :  
Filed: October 26, 2001 : Group Art Unit:  
For: SYSTEM AND METHOD FOR : Unknown  
USING AN INSTANT :  
MESSAGING ENVIRONMENT : Examiner:  
TO ESTABLISH A HOSTED : Unknown  
APPLICATION SHARING :  
SESSION :



Petition To Withdraw Notice of Omitted Items In a  
Non Provisional Application  
Under 37 C.F.R. 1.181

Assistant Commissioner for Patents  
Box DAC  
Washington, D.C. 20231

08/29/2002 MBIZUNES 00000107 10015077

01 FC:122

130.00 OP

RECEIVED

SEP 24 2002

OFFICE OF PETITIONS

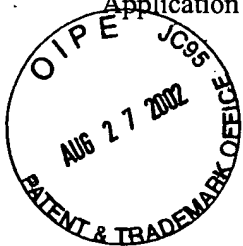
Petitioner hereby petitions the Commissioner pursuant to 37 C.F.R. § 1.181 to withdraw the Notice of Omitted Items In A Non Provisional Application regarding the above-identified patent application (the "Application") and mailed from the Patent and Trademark Office on June 27, 2002. It is petitioner's contention that the documents asserted to be missing by the Initial Patent Examining Division were submitted with the Application as originally filed on October 26, 2001.

In support of this position, a copy of the complete Application as filed is enclosed as Exhibit "A", including pages 19-23, which are alleged to have been missing. Enclosed as Exhibit "B" is a Declaration completed by Jonathan M. Darcy, an attorney with our office who was responsible for verifying the transmission of the complete Application. As asserted in the Declaration, it is the standard procedure of Mr. Darcy, as well as of every attorney in our office, to verify page by page the completeness of the contents of a patent application submission. Enclosed as Exhibit "C" is a copy of the receipt of the United States Postal Service post office at Penn Center, recording that the Express Mail envelope containing the application was received by the post office at 4:12:58 PM on October 26, 2001.

Petitioner did not receive the return receipt postcard which was submitted with the Application. A copy of the postcard as originally provided by Applicant is attached hereto as Exhibit "D". Petitioner notes that the allegedly missing pages were not noted as missing during the initial examination of the Application which resulted in the Notice to File Missing Parts of January 28, 2002, a copy of which is attached as Exhibit

"E". Significantly, the Filing Receipt of January 28, 2002, a copy of which is attached as Exhibit "F", states that "Receipt is acknowledged of this nonprovisional Patent Application." Furthermore, the Application must have been reviewed prior to the issuance of the Filing Receipt, as a foreign filing license was granted as of January 24, 2002. Accordingly, based on the foregoing, the pages were presumably not missing at the time that the application was reviewed for the First Notice to File Missing Parts, nor during review for the Foreign Filing License, otherwise the absence would have been noted and communicated.

Although Petitioner does not know where the originally submitted pages became disassociated with the filed application, the Declaration of John M. Darcy evidences that the allegedly missing pages were submitted with the rest of the Application on October 26, 2001 via Express Mail. Proof that the Patent and Trademark Office received the Application is implicit in the Office's granting of the October 26, 2001 filing date. The Filing Receipt and First Notice to File Missing Parts evidence that the complete Application was before the Initial Patent Examination Division, otherwise the missing pages would have been noted during the review for a foreign filing license, and during the review of the Application which resulted in the Notice to File Missing Parts, both of which issued on January 28, 2002. Thus, Petitioner asserts that the pages as originally filed were received by the Patent and Trademark Office, and thus the issuance of the Notice of Omitted Items In A Nonprovisional Application was in error, and should be withdrawn, and that the Application should thus be forwarded for examination.



Date: August 27, 2002

Respectfully Submitted,

Carl H. Pierce  
Registration No. 45,730  
REED SMITH LLP  
2500 One Liberty Place  
1650 Market Street  
Philadelphia, PA 19103-7301  
(215) 241-7970

RECEIVED

SEP 24 2002

OFFICE OF PETITIONS

EXPRESS MAIL CERTIFICATE (37 CFR 1.10)

Express Mail Label No. EL16682122545

Date of Deposit Aug 27, 2002

I hereby certify that this paper, and the papers and/or fees referred to herein as transmitted, submitted or enclosed, are being deposited with the U.S. Postal Service "Express Mail Post Office to Addressee" service under 37 CFR §1.10 on the date indicated above and is addressed to Assistant Commissioner for Patents, Box DAC, Washington, D.C. 20231.

Name JUDITH A. ZWEIG

Signature Judith A. Zweig



UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS  
UNITED STATES PATENT AND TRADEMARK OFFICE  
WASHINGTON, D.C. 20231  
www.uspto.gov

APPLICATION NUMBER	FILING/RECEIPT DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NUMBER
10/015,077	10/26/2001	Tod Turner	01-40169-US

07066  
REED SMITH LLP  
2500 ONE LIBERTY PLACE  
1650 MARKET STREET  
PHILADELPHIA, PA 19103

CONFIRMATION NO. 9530

## FORMALITIES LETTER



\*OC000000007371462\*

RECEIVED

SEP 24 2002

OFFICE OF PETITIONS

Date Mailed: 01/28/2002

## NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

*Filing Date Granted*

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The statutory basic filing fee is missing.  
*Applicant must submit \$ 740 to complete the basic filing fee for a non-small entity. If appropriate, applicant may make a written assertion of entitlement to small entity status and pay the small entity filing fee (37 CFR 1.27).*
- Total additional claim fee(s) for this application is \$1650.
  - \$1314 for 73 total claims over 20.
  - \$336 for 4 independent claims over 3.
- The oath or declaration is unsigned.
- To avoid abandonment, a late filing fee or oath or declaration surcharge as set forth in 37 CFR 1.16(l) of \$130 for a non-small entity, must be submitted with the missing items identified in this letter.
- **The balance due by applicant is \$ 2520.**

*A copy of this notice MUST be returned with the reply.*

Customer Service Center  
Initial Patent Examination Division (703) 308-1202

DOCKETED

PART 1 - ATTORNEY/APPLICANT COPY



#7

U.S. Patent Application  
Atty. Docket No.: 01-40169-US

**SYSTEM AND METHOD FOR  
USING AN INSTANT MESSAGING ENVIRONMENT TO ESTABLISH A  
HOSTED APPLICATION SHARING SESSION**

**Field of the Invention**

The present invention relates generally to a method for initiating an application sharing session between users in an instant messaging environment, and more particularly to using instant messaging protocols to communicate parameters for sharing a hosted  
5 application session.

**Background**

The following definitions are provided to more readily describe the present invention, and are not intended to limit the scope of the claims:

*Access Authorization* is the means by which a user's connection and request for service is *authenticated* and the user is *permitted* to access the service. There are many ways to authenticate a user, including a sign on ID and password, digital signature, electronic keycard, biometric device, etc. Once the authentication is performed, permissions may be checked to determine authorization for the request. In a secure system these connections may be usually encrypted.

A *Network Access Device* (hereafter "NAD") is any device capable of communicating over a network to one or more other *Network Access Devices* using a common protocol. Such NADs can include but are not limited to computers, servers, workstations, Internet appliances, terminals, hosts, personal digital assistants (hereafter "PDAs"), cellular telephones, etc.

An *Application Sharing Session* is defined as an application that is being accessed by two or more Network Access Devices, wherein all Network Access Devices display a common application display.

*Encryption* is the transformation of data into a form that is unreadable without requisite knowledge (a key; see below). Its purpose is to ensure privacy by keeping information hidden from anyone for whom it is not intended to access the information, even those who have access to the encrypted data.

*Decryption* is the reverse of encryption; it is the transformation of encrypted data back into a tangible form. Encryption and decryption generally require the use of some secret information, which may be referred to as a *key*.

A *Hosted Application* is an application being executed on a host and accessed by a remote Network Access Device.

A *Hosted Application Session* is a session of use of a Hosted Application.

A *Shared Application Session* is defined as a Hosted Application Session that is  
5 being concurrently accessed by more than one network access device.

Client-server computing allows distributed systems to access and transfer information via communication protocols. The Internet and many private networks use the TCP/IP suite of protocols for clients and servers to identify and locate remote systems and then establish communication sessions with those systems. A popular example of a  
10 TCP/IP network is the World Wide Web, which is a network of systems that use web servers and web browsers to move HTML documents and other content in a classic or distributed client-server model. Many business software applications require heavy data processing, which can require large amounts of data to be moved between the client and server computers. Bandwidth restrictions, upgrade costs, maintenance costs and other  
15 factors make the distributed client-server application model inappropriate for some environments, and have led to the adoption of server-based computing systems.

### The Server-Based Computing Model

In a server-based computing model, software applications are installed, maintained and supported on centrally located servers, referred to as application servers.  
20 Users access and interact with that software across a network or dialup connection using a "thin" client. In the thin client model, all of the application processing happens on the

server(s), and only user interface updates in the application are sent to the user's workstation. The input from users, including mouse movements, click events and keystrokes are captured at the users workstation and transmitted to the server where they are then passed to the target application. Application interface updates are then sent back  
5 to the client workstation for display. This process makes an application running on a remote server appear to the user as if it is running on the users workstation.

Citrix™ Independent Computing Architecture (ICA™) technology is one example of server-based computing. Users running Citrix ICA™ client software can access Citrix™ application servers. Users may then access software applications on those servers from  
10 their workstations in a server based computing model. The applications can be presented as a full graphical user interface (commonly referred to as a “desktop”) where the user has access to multiple simultaneous applications within the current session, as a published application where the user has access to just the single application that was published, or as a seamless window, where the application window is integrated into the  
15 environment of their local workstation, and the details of the application running on a remote server are hidden from the end user. Citrix ICA™ technology allows both the client and server components of client-server software applications to be loaded on Citrix application servers.

Microsoft Terminal Services™ is another example of server-based computing.  
20 Like the previous example, both the client and server components of legacy client-server software applications may be loaded on Microsoft Terminal Server™ application servers.



Users may then access those applications from their workstations in a server based computing model. The applications can be presented as a full desktop where the user has access to multiple simultaneous applications within the current session, or as a published application where the user has access to just a single application that was published.

- 5           Yet another example would be a shared X-Windows™ application or desktop in a Unix™ or Linux™ environment. While hosted application sharing can be a useful tool, it may also raise security concerns for the shared environment.

#### Network Security Concerns

- 10           The state of network security, in particular as it relates to the Internet, forces many companies and individual users to implement security systems between their private network and the public Internet in order to protect their computers from malicious use by computer "hackers", and from computer viruses, worms, and other harmful activity. These security systems are generally referred to as firewalls and take many forms in both hardware and software. They may be stateless packet filters that simply
- 15           block all activity to or from a specific Internet Protocol (hereafter "IP") address or IP port. An IP port is a sub-address of a full IP address. IP ports allow more than one connection to the same IP address for different uses. For example, an email system might communicate on one port for incoming server-to-server traffic, and use a different port for incoming user to server traffic. Firewalls may also be statefull systems that analyze
- 20           the content of the packets and the context in which they are being transmitted to decide whether the packet should be allowed. They may be implemented as software loaded on a

server, software loaded on a users workstation, dedicated hardware systems designed to handle high volumes of traffic, or some combination of devices. While these systems provide a much needed buffer between public and private networks, they can also interfere with the ability of software running on a client network to access systems on a public network by restricting access or prohibiting access completely.

### Instant Messaging & IP Networks

Instant messaging (hereafter "IM") systems employ a client-server model on IP networks to deliver text chat and other information to distributed user's in real-time.

10 Instant Messaging client software may be loaded onto a users workstation, and may allow a user to log into a remote Instant Messaging server. Once a user has logged in, business rules may be used to determine which other users are available to communicate with the first user in the instant messaging system. Many IM systems allow users to create lists of other users that they commonly communicate with. When a user in such a list logs into

15 the IM system, the server informs the list owner that a user on their list has logged on and is available to chat. In addition, Instant Messaging systems may provide directory services that permit users to search for other users. Once a user has the address of a second user, the first user can request a collaborative chat session with the second user. The second user can choose to either accept or reject the chat session. After the session

20 has been accepted, the users may be able to communicate in a private or public chat session by typing text messages to one another. The message can be either transmitted

through the IM system, or directly between users (peer to peer) once the first user has determined the availability of the second user from the IM system. These chat sessions may take place over an unsecured IP network.

#### Application Sharing Across IP Networks

5        Most application sharing technologies use IP networks to establish the shared application sessions, and may therefore be restricted by firewall systems. In a Citrix™ environment, a *Citrix ICA™ Shadow Session* is the means by which one ICA™ session can be bound to one or more other ICA™ Sessions, allowing all ICA™ sessions to display the screen of the *shadowed* users session running on a Citrix™ application server. The  
10   *shadow* user may or may not be able to send keyboard and mouse input (hereafter referred to as “actively” participating) to the remote Citrix™ application server to control the application that is being viewed depending upon whether or not they are granted permission to do so. The shadow experience may be throttled for all users by the slowest connection to the session. The Citrix™ server may be configured to listen and respond to  
15   multiple IP ports simultaneously, allowing users behind a firewall more potential ways to connect to the server, provided they know the ports that the server is listening on.

      In a Microsoft Windows Terminal Server™ environment, a hosted application session is established using the Microsoft RDP™ protocol, which uses a fixed IP port. From there, another user, with appropriate permissions, may take control of the  
20   application to allow multiple participants to show the hosted application.

### **Traditional Access to Application Sharing Sessions**

While hosted application sharing sessions provide a valuable service, the current state of the technology is limited in its ability to provide a secure, efficient or effective way for two or more users to locate each other and establish the application sharing session. The tools provided to initiate the application sharing session may not be user friendly, and may pose a security risk on a server if they enable users to access other functionality on the server, such as but not limited to: the ability to see a list of all active sessions on the server, the ability to enable or disable logons, the ability to shut down or reboot the server, the ability to install software, and other capabilities which pose a security risk. In addition, users may be impeded by firewalls or other site securing features, preventing their ability to establish a connection to the remote application server. Even if the application server has been configured to listen on multiple ports as a way to provide options to remote clients behind various firewall type devices or services, there are no client-based mechanisms that identify multiple ports and attempt to initialize an application sharing session across multiple ports.

### **Summary of the Invention**

The present invention facilitates instant messaging users in sharing applications or desktops that are running in a hosted environment, such as Microsoft Terminal Server or a Citrix environment, by facilitating the selective initiation of an application sharing

session with other instant messaging users, or by delivering other instant messaging users requests to share a hosted application.

The present invention may be embodied in a method for communicating hosted application information to allow sharing of a hosted application session. The method  
5 may include instantiating instant messaging client on a network access device engaged in a hosted application session, or on a network access device desiring to share an on-going hosted application session, and communicating from that network access device to a second access device a message indicating the desire to create a shared application session. The second network access device may be utilized to determine whether a it is  
10 desired or desirable to share the ongoing session, and communicate an acceptance or refusal of the requested sharing. The If the request is accepted, a communications path between the first and second network access devices may be utilized to communicate application sharing information to enable a hosted application session to be shared.

The present invention may alternately be embodied in a method which further  
15 includes the network access device of a user engaged in a hosted application session a request to transmit an invitation to share a session to a second network access device. Alternately, a request to be allowed to share a session can be generated at a network access device that is not engaged in a hosted application session, with the request being sent to a network access device engaged in a hosted application session.

20 The present invention may be embodied in a support service for a hosted application, wherein an accessor of the hosted application can request sharing of an on-

going application session by support entity, wherein the accessor can generate a request via an instant messaging system to the support entity to have the support entity participate in an on-going hosted application session, allowing the support entity to assist the accessor.

5

### **Brief Description of the Drawings**

The summarized description of illustrative embodiments of the present invention will be more fully understood upon a consideration of the following detailed description with reference to the attached drawings, wherein:

10           Figure 1 is an illustrative flowchart showing the present invention embodied in a User-to-User application sharing session.

Figure 2 is an illustrative flowchart showing possible details of a discovery and exchange process.

15           Figure 3 is an illustrative flowchart showing possible details of a security process for hosted sharing applications.

Figure 4 is an illustrative flowchart showing possible details of a port discovery process.

Figure 5 is an illustrative flowchart showing possible details of a notification process for hosted application sharing requests.

20           Figure 6 is an illustrative flowchart showing the present invention embodied in a support or "help-desk" embodiment.

Figure 7 is an illustrative flowchart showing the present invention embodied in a sales presentation embodiment.

Figure 8 is an illustrative flowchart showing the present invention embodied in a training environment embodiment.

5        Figure 9 is an illustration showing an overview of system components, which may be used in an embodiment of the present invention.

#### **Detailed Description of the Invention**

10        The various features and methods of this invention will now be described in the context of a collaborative hosted application sharing session, utilizing four illustrative embodiments thereof, including business collaboration, support, e-commerce sales, and training. Those skilled in the art will recognize that the inventions disclosed may also be used to begin shared sessions for a broad range of purposes. By way of example and not limitation, the disclosed methods can also be used to implement business-to-business  
15        collaboration, personal collaboration among friends, medical collaboration among doctors, and a wide variety of other implementations. Further, these methods may be implemented as a service for public consumption, or packaged as a software product that may be installed at a consumer site for private use, such as an internal intranet or private network.

20        Throughout this description, reference will be made to various implementation-specific details of illustrative collaboration environments, operating systems or platforms,

instant messaging systems, the Citrix ICA™ Protocol, Microsoft RDP™ Protocol, and the sited embodiments. These details are provided in order to illustrate embodiments of the invention, and not to limit the scope of the invention. The scope of the invention is set forth in the appended claims.

5           The instant messaging environment provides a convenient, efficient platform for two or more users to come together in a collaborative way. It offers mechanisms for users to locate other users, determine their availability, and collaborate with one another in private or public text chat. By including environment discovery and capability exchange in an instant messaging environment, this invention assists users in easily engaging in  
10   hosted application sharing sessions.

Environment discovery is the discovery of the operating environment of the network access device, including but not limited to the operating system, hardware and software components, network connectivity, etc. Network access device capability may be determined as a result of the environment discovery process.

15           Capability exchange may include, but is not limited to, the type of application sharing, a sharing protocol, and port availability information that the application server is listening on for incoming connections. This information allows instant messaging software to attempt a basic connect sequence. If a port is found that allows the correct connect sequence, then the attempt may be terminated, and software features may be  
20   enabled to allow initiation of remote application sharing sessions. If none of the ports in the list can be successfully negotiated, it may be presumed that a firewall or some other



networking issue is blocking the connection, and the application sharing launch features may be disabled for this user in this instant messaging session.

In a first embodiment of the present invention, as shown in Figure 1, two or more coworkers or cross-organization project participants may collaborate on a joint project. A first user who is accessing a session of a hosted application (an “accessor”) may instantiate an instant message session with a desired participant. Application sharing capabilities may be communicated from the accessor to the desired participant through the IM session. Additionally, an accessor in a hosted session could be able to invite other participants to join them in an application sharing session. Communication of the necessary application sharing parameters to the invited participants may be accomplished through the instant messaging software. The invited participant could receive notification of the invitation, and could accept the invitation, causing an application sharing session to be attempted. If the connection attempt were successful, the users would be joined in an application sharing session. Alternately, a minimal application sharing session could be attempted prior to the invitation being communicated to the invited participant.

Figure 1 details a process wherein a shared hosted application session between two participants is established according to the present invention. The arrows in the figures show the general flow of a process that may occur, though the exact sequence may vary due to implementation details, business requirements, or other reasons. As illustrated by Figure 1, an accessor establishes 100 or is already established in a hosted application session. The server used to deliver the hosted application session may be any

platform capable of supporting the remote application protocol in use, such as but not limited to being Citrix ICA® based, Microsoft RDP based, Unix/Linux X-Windows based, etc. The instant messaging application may either be running locally on the accessors network access device 104 or it may be running on the remote application server and delivered to the accessor in their hosted application session 102. If operating within the hosted session, the instant messaging environment may be either manually or automatically launched 102. Instant messaging software may take many forms, ranging from published standards based systems such as Internet Relay Chat (IRC) to proprietary messaging environments like America Online Instant Messenger and others. Instant messaging systems may provide presence tracking and rapid communication between two or more users. When the instant messaging software starts, an environment discovery process 108 may be performed. Such a discovery process is shown in Figure 2. Figure 2 details the environment discovery process. As shown, the Operating System (hereafter “OS”) type and version information may first be determined 202. If the OS supports remote users, 204 the session mode may be checked to see if the session is a remote session 206. The Session Mode may be defined as either *Remote* if the user is working from a separate network access device or *Local* if the user is working directly from a console directly connected to the host. A *Remote* session is any session initiated from a network access device other than the host. If the session is running as a remote session, the server may be checked to see if an application sharing user account has been configured for the server 208. If these conditions cannot be met, then the client may not

be shareable 218. If these conditions are met, then the client may be potentially shareable 210. Next, the client software may check to see if client protocol software is installed 212 on the platform. If the client protocol software is present 212, or the client is running in a remote session 214, then a flag may be set indicating that the client can join another user in a shared application 216, otherwise, the flag may be cleared indicating that the client cannot join another user 220. In short, this information may be used to determine if application sharing is possible, and in which direction. This information may be cached for later use.

Returning to Figure 1, when another instant messaging user 104 establishes a connection to the instant messaging system, their presence may be made known to the instant messaging system. Based upon rules configured in the instant messaging system and in the instant messaging clients of the instant messaging system, the presence of this new user may be shown or hidden from other users of the system. In addition, when the instant messaging software starts, an environment discovery process 106 may be performed. As discussed above, Figure 2 details the environment discovery process.

At some point, a user of the instant messaging system may decide to collaborate with another user. The first user may locate the second user using the directory service provided by a instant messaging software to locate a user they wish to collaborate with. An invitation may be sent via the instant messaging software to the target user or users, and they may accept or reject the invitation. At the point they accept the invitation 110, an instant messaging session may be created, and all users may come together into the

session to collaborate using text based chat and/or possibly voice/video chat. The method in which they chat may be determined by the capabilities of the instant messaging platform.

When an instant messaging session is established, the permissions of each user in the session may be verified 112 to see if they are permitted to initiate an application sharing session with another user, or if they are permitted to share hosted applications to remote users. If a user is permitted 114, the remote configuration information may be passed between the users in the session to determine the platform and ability of each user in the session.

As shown in Figure 2, when a user enters an instant messaging session, a capabilities exchange may occur to see if that user and session is running as a remote session 224. First, the local share ability 226 may be determined by checking the 'can share' flag 216. If application sharing is supported locally 226, then the remote user capabilities may be checked to see if they can host an application sharing session 228. If the remote user can host an application sharing session 228, then a security process 230 may be performed to see if the application sharing session may be established according to permissions and business rules.

A variety of security features may be implemented, including encryption of the application sharing parameters that are passed between instant messaging clients and the destruction of those parameters after their use, and an opaque way of exposing the application sharing parameters to the instant messaging clients such that users do not see

the actual commands, accounts, and passwords used to establish the session. This may allow an Application Server Administrator to configure accounts used to enable application-sharing sessions without publishing the details to the end users. If a user of the system is terminated, no security risk is present because the user was never shown the details necessary to establish the application sharing session. Since information may be fetched each time the user connects to the system, an administrator can maintain and change the accounts at any time without needing to notify the end users of the change. The next time a user connects to the system, new parameters will be used automatically.

An additional feature may be the ability to configure which users have permission to share hosted applications, the permitted direction of the application sharing session request (hosted user to remote user, remote user to hosted user, either, or neither), whether notification will be provided to a hosted user, and whether a hosted user must accept the request before the application sharing session may be instantiated. Existing settings for the application server software may be accommodated such that if notifications are enabled, a user may not be issued an application sharing request dialog twice, once from the instant messaging software, and once from application server.

An instant messaging system may be extended such that user settings, contact lists, preferences, and profiles may be stored on an instant messaging server. Such a process allows a user to connect from any NAD, or to any application server while seeing the same user settings, contact lists, preferences, and profile.

Figure 3 shows details associated with a security process. First, a company profile 300 may be checked to see if the company permits application sharing 302. If application sharing is permitted, a local user profile may be checked 304 to see if the user may join another user's hosted application session 306. If local user is permitted to join the session 5 of another user, then the remote user's profile may be checked 308 to see if users are permitted to share their application with them. If other users are permitted to join the session 310 then access rights may be granted 312. If any of these validations fail, then rights may be denied 314.

Returning to Figure 2, if a user is denied rights to share an application 232, then 10 the application sharing features may be disabled in the instant message client while that remote user is selected 242. If the user is granted rights to share the application 232, then the instant messaging client may perform the Port Discovery process 234 as described further below in Figure 4. If the Port discovery process is successful, 236, then application-sharing features may be enabled in the instant message client while that 15 remote user is selected 240.

Returning to Figure 1, if a user has permission to join an application session another user, and has the application sharing client software installed on their NAD, then the instant messaging software may send a request to the accessor of the hosted application to retrieve the configured application sharing parameters. The hosted client 20 may encrypt the application sharing parameters needed for establishing a session and transmit them through the instant messaging system 116 to the remote user. This

information may include but is not limited to server address, session ID, a list of ports that the server is listening on, user account information, user password, screen settings, and other settings that may be needed for the application sharing protocol in use. When the remote user instant messaging software receives this information, it may begin a  
5 background process, 118, of determining if a user is able to connect to the remote application session 120. Application sharing parameters may be masked from the user while they are present on a NAD. Masking is defined as a process(es) or lack of a process that limits a user's ability to perceive application-sharing parameters.

As shown, Figure 4 details a port discovery process. When the application sharing  
10 parameters are extracted from a communicated packet 400, the process may check to see if this is the first time a port discovery has been run from this client session 402. If this is not the first discovery process, a cache may be checked 404 to see if a port discovery process has already been performed for this server. If a port needs to be discovered, a list of ports may be extracted from a communicated data packet. For each port in the list, an  
15 attempt may be made to establish a application sharing connection to the server 406. If the connection cannot be established 408, then a next listed port may be processed 410. This procedure may continue until a successful connection occurs, or until the last port in the list is checked. If no valid ports could be located, the application sharing ability may be turned off in the user interface 414. If a valid port is located, the server and port  
20 information may be updated in the local cache 412, and the application sharing ability may be enabled in the user interface 416.

In Figure 1, this port discovery process is summarized in items 118, 120, 122, and 130. Since it is feasible for a hosted user to 'push' the application sharing command to a remote user, it may be possible for either a hosted user, or a remote user, to initiate the application sharing session 124. In any case, when the application sharing session is initiated, a notification process may be performed 126. Application sharing parameters may be masked from the user while they are using an NAD.

Figure 5 details a notification process. If a remote user initiates an application sharing request 500, then a notification feature built into an application server may be verified on the user account. If a notification is enabled 502, the application server may be allowed to perform a normal notification and or rejection process 514. If the application server notification is not enabled, then the settings of the user profile in the instant messaging system may take over and be checked 504. If application-sharing notification is enabled 506, then an application-sharing request may be sent to the user of the hosted application 508. If the hosted user accepts the request 510, or if application-sharing notification is not enabled 506, then the application sharing session may be established without further delay 516. Otherwise, the remote user may be notified that the hosted user denied the request 512, and the application sharing session may not be initiated.

In Figure 5, if a hosted application user pushes an application-sharing request to a desired participant 518, then the desired participant may be given the opportunity to accept the session 520. If the desired participant accepts the request, the session may be



started 522. If the desired participant rejects the request, then the hosted application user may be notified that sharing was rejected 524.

In Figure 1, this notification process and session establishment is summarized in items 126 and 128. The final process in establishing the application sharing session  
5 may include destroying the connection parameters used to create the session 132. This action ensures that the connection parameters are not left on a user's system where they could be exploited for inappropriate or unauthorized activities.

Although the example provided illustrates the present invention in terms of a hosted application session user inviting another desired participant into a session, a  
10 different user may desire to interject him or herself into an on-going hosted application session of another. In this case, the interjector may request of the on-going user information to allow the interjector to interject. Such a request may also be referred to as a pull, where the interjector pulls the information from the on-going user.

In another embodiment, this invention may be used to facilitate a help desk  
15 environment. A help desk is a common way to provide centralized assistance and training for, but not limited to, users, software, computers and other NADs. In a support desk embodiment, a support person may monitor an instant messaging system to receive help requests. When a user of a hosted application requests help through the instant messaging software, they may be connected to an available support person, providing immediate  
20 support. Application sharing parameters may be communicated from the user session to the support person's instant messaging interface, allowing an instant messaging interface

time to determine the feasibility of establishing an application sharing session. A support person could engage a user in instant text messaging to discover the extent of the users problem or request. If feasible, the support person could offer to take control of the application and assist the user directly. If the user agrees, the support person could  
5 initiate the application sharing session and directly assist the user of the hosted application, thereby reducing support time, and increasing user satisfaction. A variation of this may be implemented wherein a user initiates an application sharing session by pushing a request to a support person, causing the support person's interface to enter an application sharing session. This variation would place a user in control of when/if a  
10 support person could ever directly access a hosted application being worked on.

As shown in Figure 6, a user of a hosted application may use an IM system to request help from a support person at a help desk. The arrows in the figures show the general flow of the process that occurs, though the exact sequence might be different due to implementation details or business requirements. A user may establish 600 or may  
15 already have established a hosted application session. While operating within a hosted session, an instant messaging environment may be either manually or automatically launched 602. When the instant messaging software starts, an environment discovery process 604 may be performed.

When a support user 608 establishes a connection to an instant messaging system,  
20 their presence may be made available to the instant messaging system. When the instant messaging software starts, an environment discovery process 610 may be performed.

The hosted user may next use the instant messaging software to initiate a help request 606. The request may be directly routed to a support person or placed in a support queue. A support person may then address the help request from the queue, and initiate an instant messaging session. An instant messaging session may thus be created 612, 5 bringing the user and the support person together into a session to collaborate using text based chat or possibly voice/video chat. The chat medium may be determined by the capabilities of the instant messaging platform.

Once an instant messaging session is established, the permissions of the user and the support person in the session may be verified 614 to see if the user and/or the support 10 person are permitted to initiate a remote application sharing session. If permitted 616, the remote configuration information may be passed between the user and the support person in the session to determine the platform and ability of each person in the session.

A capability discovery and exchange process is shown in greater detail in Figure 2. When a user is selected in the instant messaging session, a capabilities exchange may 15 occur to see if that user and session is running as a remote session 224. The local share ability 226 may be determined by checking a 'can share' flag 216. If application sharing is supported locally 226, then remote user capabilities may be checked to see if they may support an application sharing session 228. If the remote user may support an application sharing session 228, then a security process 230 may be performed to see if an 20 application sharing session may be established according to permissions and business rules.

Figure 3 illustrates details which may be associated with a security process. A company permits application sharing 302. If application sharing is permitted, a local user profile may be checked 304 to see if a first user may join another (second) user's hosted application session 306. If the first user is permitted to join the session, the second user's profile may be checked 308 to determine whether the second user is permitted to share a hosted application session. If sharing is permitted 310 then sharing rights may be granted 312. If any of these validations fail, sharing rights may be denied 314.

As shown in Figure 2, if the second user second is denied rights to share an application 232 to a first user, then the application sharing features may be disabled in the instant message client while that first user is selected 242. If the second user is granted rights to share the application 232, then the instant messaging client may perform a port discovery process 234 as described further in Figure 4. If the Port discovery process is successful, then application-sharing features may be enabled in the instant message client while that remote user is selected 240 upon affirmative establishment of an application sharing session 236.

Returning to Figure 6, if a support person has permission to initiate an application sharing session with a hosted application user, and has adequate application sharing client software installed on their NAD, then the instant messaging software may be used to send a request to the hosted application user to obtain the configured application sharing parameters. Parameter needed for establishing an application sharing session may be encrypted and transmitted through the instant messaging system 618 to the support users

instant messaging client. This information may include a server address, session ID, list of ports that the server is listening on, user account, user password, screen settings, and other settings that may be necessary for establishing an application sharing session. When a support users instant messaging software receives this information, it may begin  
5 a background process of determining if the support user is able to connect to the remote user session 620.

In Figure 6, a port discovery process is summarized in items 618, 620, 622, 624, and 632. A more full description of a port discovery process is described with regards to Figure 4, discussed above. When the application sharing session is initiated 626, a  
10 notification process may be performed 628.

Figure 5 shows details associated with notification process. If a remote user initiates an application-sharing request 500, a notification feature built into the application server may be checked to determine if notification is enabled for user account. If the notification is enabled 502, the application server may perform a normal  
15 notification and or rejection process 514. If the application server notification is not enabled, then the settings of the user profile in the instant messaging system may be used to determine notification parameters 504. If application-sharing notification is enabled 506, then an application-sharing request may be sent to the user of the hosted application 508. If the hosted user accepts the request 510, or if application-sharing notification is not  
20 enabled 506, then the application sharing session may be established without further

delay 516. Otherwise, the remote user may be notified that the hosted user denied the request 512, resulting in the application sharing session not being initiated.

If a hosted user "pushes" an application-sharing invitation to a remote user 518, the remote user may be given the opportunity to accept the session invitation 520. If the user accepts the invitation, the session may be started 522. If the user rejects the invitation, then the hosted user may be notified that the remote session was rejected 524.

In Figure 6, this notification process and session establishment is summarized in items 628 and 630. The final process in establishing the application sharing session may include destroying the connection parameters used to create the session 634. This action ensures that the connection parameters are not left on a user's system where they could be exploited for inappropriate or unauthorized activities.

In another embodiment of this method, a user may be connected to a hosted application for purposes of a demonstration. When that user connects to the hosted application, they could be placed in an instant message session, which could notify a sales person that a user was viewing their software in real-time. In addition, the application sharing parameters could be communicated from the user session to the sales person's instant messaging interface seamlessly in the background, allowing the instant messaging interface time to determine the feasibility of establishing an application sharing session. The sales person could engage the user in instant text messaging, and offer to demonstrate the application to the user. If the user agrees, the sales person could initiate the application sharing session and 'walk' the user through the features of the

hosted application, thereby increasing the effectiveness of the demonstrator's presentation.

Figure 7 details such an embodiment. The sales person may use the collaborative environment to proactively assist the customer with the demonstration, answer questions interactively, and highlighting the features of the application. As illustrated in Figure 7, a user may establish 700 or already be established in a hosted application session that may be running a demonstration. While operating within the hosted application session, the instant messaging environment may be automatically launched 702. When the instant messaging software starts, an environment discovery process 704 may be performed.

When a sales person 708 establishes a connection to the instant messaging system, their presence may be made known to the instant messaging system. Based upon rules configured in the instant messaging system and in the instant messaging clients of the instant messaging system, the presence of this new user may be shown or hidden from other users of the system. In addition, when the instant messaging software starts, an environment discovery process 710 may be performed.

When a prospect enters a hosted environment for a demonstration, a sales person may be notified of the presence 706. Either the prospect or the sales person may initiate collaboration. If the prospect initiates collaboration, the request may be queued up for an available sales person. If a sales person initiates collaboration, instant messaging may begin immediately. An instant messaging session may be created 712, bringing the prospect and the sales person together into an IM session to collaborate using text based

chat or voice/video chat. The method in which they chat may be determined by the capabilities of the instant messaging platform.

Once an instant messaging session is established, permissions of the prospect and the sales person in the session may be verified 714 to see if they are permitted to initiate a remote application sharing session. If permitted 716, remote configuration information may be passed between the NAD's of the prospect and the sales person in the session to determine the platform and ability of each NAD.

In Figure 7, if a sales person has permission to share the hosted application of a prospect, and has sufficient application sharing client software installed on their NAD 716, then the instant messaging software may send a request to the prospect that is hosted to retrieve the application sharing parameters. The hosted prospects instant messaging client may encrypt the application sharing parameters needed for establishing a session and transmit them through the instant messaging system 718 to the sales person. This information may include the server address, session ID, list of ports that the server is listening on, user account, user password, screen settings, and other settings that may be necessary for establishing an application sharing session. When the sales person's instant messaging software receives this information, it may begin a background process of determining if the sales person is able to connect to the hosted application server 720.

In Figure 7, a port discovery process is summarized in items 718, 720, 722, 724, and 732. If application sharing is feasible, the application-sharing launch features may become enabled in the instant messaging software. The sales person may then initiate an



application sharing session 726 to assist the prospect interactively during the sales process 728. In this manner, a personal touch is brought to the sales process in an e-commerce environment. The final process in establishing such an application sharing session may include destroying the connection parameters used to create the session 730.

- 5 This action ensures that the connection parameters are not left on a sales persons system where they could be exploited for inappropriate or unauthorized activities.

In another embodiment, a trainer may host a moderated training session with one or more users. The trainer could invite the trainees to a moderated instant messaging session, then push the hosted application sharing parameters through the instant  
10 messaging system to the trainees' instant messaging client. The instant messaging client could receive the command and begin the process of connecting each of the trainees to the instructor's hosted application session via an application sharing capability. As each trainee is joined to the session, a user status indicated by the instant messaging system could be updated to show whether the trainee is connected read-only or interactively to  
15 the trainers session. Requiring users that participate in the application sharing session to use NAD's meeting minimum bandwidth, screen resolution, and other performance requirements before a session is established may further enhance the training experience by minimizing delays inherent in the use of slower equipment. The status of users that failed to connect due to a performance restriction could be indicated in the trainer's  
20 instant messaging software such that the trainer knew the reason and could either reduce

the requirements, thereby allowing the user to join the session, or explain to the trainee that they will have to reschedule the training.

Figure 8 details such an embodiment in which a trainer hosts an interactive training session for one or more users in a hosted application environment. The trainer may use the collaborative environment to create a moderated training session for the students. The trainer may first enter a hosted application environment and prepare it for the training session 800, thus ensuring that the application is configured correctly. Once the environment is configured, the trainer may create a moderated conference in the instant messaging platform 802. The trainer may specify the minimum requirements for participants in the training session 804, which may include the video resolution and bandwidth.

The affect that the performance characteristics of a NAD have on a shared hosted application session is driven by the poorest capability of a sharing NAD in the environment. If one NAD is connected via a slow network connection, each other participant in the session must await while communication on the slowest network connection is completed. Alternately, a NAD having sub-standard graphics capability may result in a hosted application session being generated at a low resolution to accommodate the NAD having sub-standard graphics, or alternately being generated at full resolution, requiring a user of the NAD to continuously scroll around a display, delaying the users participation in a collaborative session. Other parameters, such as whether a display is presented in color, whether a processor or memory limitation of a

NAD adversely effects the pace of the session, or whether a particular NAD has audio capability can adversely impact the collaborative nature of a shared application session, thus creating an incentive to limit participation of such a sub-standard NAD during a session.

5           Once the environment has been setup, the trainer may send an invitation to desired participants, allowing them to join the moderated conference 806. The instant messaging system may forward the invitations to each participant. When a desired participant's instant messaging client receives the invitation, 808, it may first check the minimum requirements 810 to see if the NAD on which it is resident will be permitted in  
10   the conference. If the NAD does not meet the minimum requirements, the reason for the restriction may be displayed to the desired participant 812, and the user's conference status may be updated to indicate that they are not participating in the conference. The reason for the users non-participation may be included in status information that is available to the trainer, allowing the trainer to reduce the minimum requirements, and  
15   resend the invitation to the failed desired participants if desired.

          If the minimum requirements were met, the application sharing parameters may be encrypted and may be sent to the remote trainees' NADs 814. When the instant messaging client receives this information, it may begin a process to verify application sharing potential 816.

20           If a port discovery process results in a determination that no valid port was located 818, a user may be notified, and their conference status updated to show that they

are not participating in an application sharing session 828. If a user can participate in the application sharing session, they may be prompted to join the training session 820. If a user chooses to participate 822, the application sharing session may be launched, 824, and the user's conference status updated to show that they are now participating 826. The  
5 final process in establishing the application sharing session may include destroying the connection parameters used to create the session 830. This action ensures that the connection parameters are not left on a user's system where they could be exploited for inappropriate or unauthorized activities. If the user chooses not to participate 822, the users conference status may be update to show they are not participating, and the reason  
10 may be set to indicate the user declined to participate 828.

From the foregoing teachings, it can be appreciated that a new, novel and non-obvious method for establishing hosted application sharing sessions using an instant messaging environment has been disclosed. For reference, Figure 9 is provided as an example system component overview which may be used in an embodiment of the  
15 present invention. It is to be understood that numerous alternatives and equivalents will be apparent to those of ordinary skill in the art, given the teachings herein, such that the present invention is not to be limited by the foregoing description but only by the appended claims.

## **Claims**

What is claimed is:

- 5           1)     A method for communicating hosted application information to allow  
sharing of a hosted application session, comprising the steps of:
- instantiating a first instant messaging client on a first network access device, said  
first network access device being remote from a hosted application server, said first  
network access device participating in a hosted network application;
- 10           establishing a communications path from the first network access device to a  
second network access device, said second network access device running a second  
instant messaging client, said second instant messaging client being communicably  
connected to said first instant messaging client via a network, said communications path  
for communicating information using an instant messaging protocol between the first and
- 15           second network access devices; and
- using an instant messaging protocol to communicate hosted application  
information to the second network access device, said information comprising parameters  
for sharing the hosted application session being participated in by the first network access  
device.

20

2) A method for communicating hosted application information to allow sharing of a hosted application session according to claim 1, wherein said hosted application information comprises port information for accessing a hosted application session to be shared.

5

3) A method for communicating hosted application information to allow sharing of a hosted application session according to claim 1, wherein said hosted application information comprises protocol information for accessing a hosted application session to be shared.

10

4) A method for communicating hosted application information to allow sharing of a hosted application session according to claim 1, wherein said hosted application information comprises access authorization information for accessing a hosted application session to be shared.

15

5) A method for communicating hosted application information to allow sharing of a hosted application session according to claim 1, wherein said hosted application information is masked to prevent said information from being readily discernible by a user of the first or second network access device.

20

6) A method for communicating hosted application information to allow sharing of a hosted application session comprising the steps of:

instantiating a first instant messaging client on a first network access device, said first network access device being remote from a hosted application server, said first

5 network access device participating in a hosted network application;

establishing a communications path from the first network access device to a second network access device, said second network access device running a second instant messaging client, said second instant messaging client being communicably connected to said first instant messaging client via a network; and

10 receiving a request to issue an invitation from the first network access device to the second network access device, said invitation inviting a user of the second network access device to participate in a shared hosted application session through the second network access device.

15 7) A method for communicating hosted application information to allow sharing of a hosted network application session according to claim 6, further comprising the step of determining whether a hosted application is shareable before issuing an invitation to the second network access device.

20

8) A method for communicating hosted application information to allow sharing of a hosted network application session according to claim 7, wherein the step of determining whether a hosted application session is shareable comprises determining whether the hosted application server is capable of supporting a shared hosted application session.

9) A method for communicating hosted application information to allow sharing of a hosted network application session according to claim 6, further comprising the step of determining whether the second network access device is capable of participating in a shared hosted application session before allowing an invitation to be communicated to the second network access device.

10) A method for communicating hosted application information to allow sharing of a hosted network application session according to claim 9, wherein the step of determining whether the second network access device is capable of participating in a shared hosted application session comprises determining whether the second network access device has compatible hosted application sharing software installed.



11) A method for communicating hosted application information to allow sharing of a hosted network application session according to claim 9, wherein the step of determining whether the second network access device is capable of participating in a shared hosted application session comprises determining whether the second network access device is able to access the hosted application server in accordance with hosted application information communicated to the second network access device.

12) A method for communicating hosted application information to allow sharing of a hosted network application session according to claim 11, wherein the step of determining whether the second network access device is able to access the hosted application server comprises instantiating a server access attempt from the second network access device to the hosted application server to determine whether the second network access device is capable of communicating with a port on a hosted application server in accordance with the hosted application information.

15

13) A method for communicating hosted application information to allow sharing of a hosted network application session according to claim 6, further comprising the step of determining whether a network access device should be invited to share a hosted application session, said determination being dependant upon the performance capability of the network access device.

20

14) A method for communicating hosted application information to allow sharing of a hosted network application session according to claim 13, wherein the determination is dependant upon a graphical display resolution of the network access device.

5

15) A method for communicating hosted application information to allow sharing of a hosted network application session according to claim 13, wherein the determination is dependant upon the bandwidth of the network connection between the network access device and the hosted application server.

10

16) A method for communicating hosted application information to allow sharing of a hosted application session according to claim 6, further comprising the step of communicating hosted network application information to the second network access device, wherein said hosted network application information is masked to prevent said information from being readily discernible by a user of the second network access device.

15

17) A method for communicating hosted application information to allow sharing of a hosted application session according to claim 16, wherein said hosted application information is encrypted while being communicated to the second network access device.

20

18) A method for communicating hosted application information to allow sharing of a hosted application session according to claim 16, wherein said hosted application information comprises access authorization information.

5 19) A method for communicating hosted application information to allow sharing of a hosted application session according to claim 16, wherein said access authorization information is unique to a hosted application sharing session.

20) A method for communicating hosted application information to allow  
10 sharing of a hosted application session according to claim 16, wherein said hosted application information is communicated to said second network access device via said first network access device, and further wherein said hosted application information is masked to prevent said information from being readily discernible by a user of the first network access device.

15

21) A method for communicating hosted application information to allow sharing of a hosted application session according to claim 6, wherein said hosted application information comprises role information for defining a participants authority to interact with a shared hosted application.

20

22) A method for communicating hosted application information to allow sharing of a hosted application session according to claim 21, wherein said role information may be used to alternate control of a shared hosted application session between a first network access device and a second network access device.

5

23) A method for communicating hosted application information to allow sharing of a hosted application session according to claim 21, wherein a user is associated with a network access device, said user having an identity, and wherein said role information is dependant on the identity of the user.

10

24) A method for communicating hosted application information to allow sharing of a hosted application session comprising the steps of:

instantiating a first instant messaging client on a first network access device, said first network access device being remote from a hosted application server,  
5 said first network access device participating in a hosted network application;

establishing a communications path from a second network access device to the first network access device, said second network access device having a second network connection, said network connection having a band width, said second network access device further running a second instant messaging client, said second instant  
10 messaging client being communicably connected to said first instant messaging client via the network connection, said communications path for communicating hosted application information using an instant messaging protocol between the first and second network access devices; and

receiving at the first network access device a request from the second  
15 network access device, said request requesting communication of hosted network application information to the second network access device to allow the second network access device to participate in a shared hosted application session.

25) A method for communicating hosted application information to allow sharing of a hosted network application session according to claim 24, further comprising the step of determining whether a hosted application can be shared before communicating hosted application information to the second network access device.

5

26) A method for communicating hosted application information to allow sharing of a hosted network application session according to claim 25, wherein the step of determining whether a hosted application session can be shared comprises determining whether the hosted application server is capable of supporting a shared hosted application session.

10

27) A method for communicating hosted application information to allow sharing of a hosted network application session according to claim 25, further comprising the step of determining whether the second network access device is capable of participating in a shared hosted application session before communicating hosted application information to the second network access device.

15

28) A method for communicating hosted application information to allow sharing of a hosted network application session according to claim 27, wherein the step of determining whether the second network access device is capable of participating in a shared hosted application session before communicating hosted application information to the second network access device comprises determining whether the second network access device has compatible hosted application sharing software installed.

29) A method for communicating hosted application information to allow sharing of a hosted network application session according to claim 27, wherein the step of determining whether the second network access device is capable of participating in a shared hosted application session before communicating hosted application information to the second network access device comprises determining whether the second network access device is able to access the hosted application server in accordance with hosted application information communicated to the second network access device.

15

30) A method for communicating hosted application information to allow sharing of a hosted network application session according to claim 29, wherein the step of determining whether the second network access device is able to access the hosted application server comprises instantiating a server access attempt from the second  
5 network access device to the hosted application server to determine whether the second network access device is capable of communicating with a port on a hosted application server in accordance with the hosted application information.

31) A method for communicating hosted application information to allow  
10 sharing of a hosted network application session according to claim 24, further comprising the step of determining whether hosted application information should be communicated to the second network access device in response to a request, said determination being dependant upon the performance capability of the second network access device.

15 32) A method for communicating hosted application information to allow sharing of a hosted network application session according to claim 31, wherein the determination is dependant upon the graphical display resolution of the network access device.



33) A method for communicating hosted application information to allow sharing of a hosted network application session according to claim 31, wherein the determination is dependant upon the bandwidth of the second network connection.

5           34) A method for communicating hosted application information to allow sharing of a hosted application session according to claim 24, further comprising the step of communicating hosted application information to the second network access device, wherein said hosted application information is masked to prevent said information from being readily discernible by a user of the second network access device.

10

35) A method for communicating hosted application information to allow sharing of a hosted application session according to claim 34, wherein said hosted network application information is encrypted while being communicated to the second network access device.

15

36) A method for communicating hosted application information to allow sharing of a hosted application session according to claim 34, wherein said hosted application information is communicated to said second network access device via said first network access device, and further wherein said hosted application information is  
20 masked to prevent said information from being readily discernible by a user of the first network access device.

37) A method for communicating hosted application information to allow sharing of a hosted application session according to claim 34, wherein said hosted application information comprises access authorization information.

5

38) A method for communicating hosted application information to allow sharing of a hosted application session according to claim 37, wherein said access authorization information is unique to a hosted application sharing session.

10

39) A method for communicating hosted application information to allow sharing of a hosted application session according to claim 24, wherein said hosted application information comprises role information, said role information defining the authority of a network access device to interact with a shared hosted application.

15

40) A method for communicating hosted application information to allow sharing of a hosted application session according to claim 39, wherein said role information is used to alternate control of a shared hosted application session between a first network access device and a second network access device.

41) A method for communicating hosted application information to allow sharing of a hosted application session according to claim 39, wherein a user is associated with a network access device, said user having an identity, and wherein said role information is dependant on the identity of the user.

5

42) A method for providing assistance for a hosted application to an accessor of the hosted application from a support network access device, comprising the steps of:  
instantiating an instant messaging client on a network access device being used by the accessor;

10 instantiating an instant messaging client on a support network access device;  
receiving a support request from the accessor network access device, said accessor network access device accessing a hosted application from a remote location, said request being a request for assistance for an on-going hosted application session;  
communicating to the support network access device hosted application  
15 information using an instant messaging protocol, said hosted application information comprising information for allowing the support network access device to share the on-going hosted application session; and  
instantiating an access to the on-going hosted application session on the support network access device, said access causing the hosted application session to become  
20 shared with the support network access device.

43) A method for providing accessor assistance for a hosted application according to claim 42, wherein the hosted application information comprises port identification information, said port identification information comprising identification of at least one port on a hosted application server, said hosted application server hosting  
5 the on-going hosted application session.

44) A method for providing accessor assistance for a hosted application according to claim 42, wherein the hosted application information comprises role information, said role information defining the authority of a network access device to  
10 interact with a shared hosted application.

45) A method for providing accessor assistance for a hosted application according to claim 44, wherein said role information may be used to alternate control of a shared hosted application session between said accessor network access device and said  
15 support network access device.

46) A method for providing accessor assistance according to claim 48, wherein an accessor is associated with the accessor network access device, said accessor having an identity, and wherein said role information is dependant on the identity of the  
20 accessor.

47) A method for providing accessor assistance for a hosted application according to claim 42, wherein said hosted application information is masked to prevent said information from being readily discernible by a user of the support network access device.

5

48) A method for providing customer assistance for a hosted application according to claim 42, wherein said hosted application information is masked to prevent said information from being readily discernible by a user of the accessing network access device.

10

49) A method for providing accessor assistance for a hosted application according to claim 42, wherein said hosted network application information is encrypted while being communicated to the support network access device.

15

50) A method for providing accessor assistance for a hosted application according to claim 42, wherein said hosted application information comprises access authorization information.

51) A method for providing accessor assistance for a hosted application according to claim 50, wherein said access authorization information is unique to the support request.

20

52) A method for providing a hosted application training session, said training session including shared access to a hosted application session between at least one trainer and at least one trainee, said method comprising the steps of:

5       instantiating a hosted application session from a trainer's network access device, said hosted application session hosted by a remote hosted application server, said trainer's network access device being connected to a communications network, said remote hosted application server also being connected to the network;

          instantiating an instant messaging client on the at least one trainer's network  
10   access device;

          instantiating an instant messaging client on at least one trainee's network access device, said network access device having a trainee's connection to the communications network, said trainee's network connection having a bandwidth;

          communicating to the at least one trainee's network access device a capability  
15   verification request;

          determining whether said at least one trainee's network access device is capable of participating in a shared hosted application training session; and

          when it is determined that said at least one trainee's network access device is capable of participating in a shared hosted application session, communicating to the at  
20   least one trainee's network access device hosted application information, said hosted

application information comprising information allowing the at least one trainee's network access device to share a hosted application training session.

53) A method for providing hosted application information to enable a hosted application training session according to claim 52, wherein said capability verification request comprises application server port information, and wherein said determination of whether said at least one trainee's network access device is capable of participating in a shared hosted application training session comprises determining whether the at least one trainee's network access device is capable of communicating with the hosted application server via the application server port information.

54) A method for providing hosted application information to enable a hosted application training session according to claim 52, wherein performance capabilities of a trainee's network access device affect performance of a shared application training session, said effect being quantifiable as an amount, wherein said determination of whether said at least one trainee's network access device is capable of participating in a shared hosted application training session is dependant on the amount that said at least one trainee's network access device will restrict performance of the shared hosted application session.

20

55) A method for providing hosted application information to enable a hosted application training session according to claim 54, wherein performance capabilities of a trainee's network access device affect performance of a shared application training session, said effect being quantifiable as an amount, wherein the amount that said at least one trainee's network access device will restrict performance of the shared hosted application session is dependant on the bandwidth of the at least one trainee's network connection.

56) A method for providing hosted application information to enable a hosted application training session according to claim 54, wherein performance capabilities of a trainee's network access device affect performance of a shared application training session, said effect being quantifiable as an amount, wherein the amount that said at least one trainee's network access device will restrict performance of the shared hosted application session is dependant on an ability of the trainee's network access device to display information associated with the hosted application session.

15

57) A method for providing hosted application information to enable a hosted application training session according to claim 52, wherein said determination of whether said at least one trainee's network access device is capable of participating in a shared hosted application training session comprises determining whether the at least one trainee's network access device has adequate software installed to allow said at least one trainee's network access device to share a hosted application session.

20



58) A method for providing hosted application information to enable a hosted application training session according to claim 52, wherein the step of communicating to said at least one trainee's network access device a capability verification request occurs in response to a request from the at least one trainee's network access device to participate in a shared hosted application training session.

59) A method for providing hosted application information to enable a hosted application training session according to claim 52, wherein the step of communicating to said at least one trainee's network access device a capability verification request occurs in response to a request from the at least one trainer's network access device to invite a user to participate in a shared hosted application training session.

60) A method for providing hosted application information to enable a hosted application training session according to claim 52, wherein the step of communicating to said at least one trainee's network access device a capability verification request further comprises masking the capability verification request such that it is not readily discernible to a user of said at least one trainee's network access device.

61) A method for providing hosted application information to enable a hosted application training session according to claim 52, wherein the step of communicating to said at least one trainee's network access device a capability verification request further comprises the step of encrypting the capability verification request prior to  
5 communicating the capability verification request to said at least one trainee's network access device.

62) A method for providing hosted application information to enable a hosted application training session according to claim 52, wherein the step of communicating to  
10 said at least one trainee's network access device hosted application information further comprises masking the hosted application information such that it is not readily discernible to a user of said at least one trainee's network access device.

63) A method for providing hosted application information to enable a hosted  
15 application training session according to claim 52, wherein the step of communicating to said at least one trainee's network access device hosted application information further comprises the step of encrypting the hosted application information prior to communicating the capability verification request to said at least one trainee's network access device.

20

64) A method for providing hosted application information to enable a hosted application training session according to claim 52, wherein said hosted application information for allowing said at least one trainee's network access device to share a hosted application training session further comprises role information, said role information defining authority of a network access device to interact with a shared hosted application training session.

65) A method for providing hosted application information to enable a hosted application training session according to claim 64, wherein said role information is used to alternate control of a shared hosted application session between a trainer's network access device and a trainee's network access device.

66) A method for communicating hosted application information to allow sharing of a hosted application session according to claim 64, wherein at least one trainee is associated with said at least one trainee's network access device, said at least one trainee having an identity, and wherein authority associated with said role information is dependant on the identity of the at least one trainee.

67) A method for communicating hosted application information to allow sharing of a hosted application session according to claim 64, wherein at least one trainer is associated with said at least one trainer's network access device, said at least one trainer having an identity, and wherein authority associated with said role information is  
5 dependant on the identity of the at least one trainer.

68) A method for providing a shared hosted application session, wherein said session is shared among a plurality of shared hosted application participants; comprising the steps of:

10 instantiating a hosted application session on a first network access device associated with a first application participant, said hosted application session being hosted by an application hosting server;

instantiating an instant messaging client on said first network access device;

using said instant messaging client to establish a communications path to at least a  
15 second network access device associated with at least a second participant, said second network access device having a second connection to the network, said second network connection having a bandwidth;

communicating to said at least second network access device a capability verification request;

20 determining whether said second network access device is capable of participating in a shared hosted application session;

when it is determined that said second network access device is capable of participating in a shared hosted application session, communicating to the at least second participant via the communications path an invitation to share the hosted application session;

5       when it is determined that said second network access device is capable of participating in a shared hosted application session, determining whether the at least second participant desires to participate in a shared hosted application session;

10       when it is determined that said second network access device is capable of participating in a shared hosted application session and that said at least second participant desires to participate in a shared hosted application session, communicating to said second network access device hosted application information, said hosted application information for allowing said second network access device to share a hosted application session; and

15       when it is determined that said second network access device is capable of participating in a shared hosted application session and that said at least second participant desires to participate in a shared hosted application session, instantiating an access to the shared application session on said at least second network access device in accordance with the communicated hosted application information.

69) A method for providing a shared hosted application session according to claim 68, wherein said capability verification request comprises application server port information, and wherein said determination of whether said second network access device is capable of participating in a shared hosted application session comprises  
5 determining whether said second network access device is capable of communicating with the hosted application server via the application server port information.

70) A method for providing a shared hosted application session according to claim 68, wherein performance capabilities of a network access device affect  
10 performance of a shared application session, said effect being quantifiable as an amount, wherein said determination of whether said second network access device is capable of participating in a shared hosted application session is dependant on the amount that said second network access device will restrict performance of the shared hosted application session.

15

71) A method for providing a shared hosted application session according to claim 70, wherein the amount that said second network access device will restrict performance of the shared hosted application session is dependant on the bandwidth of the second network connection.

20

72) A method for providing a shared hosted application session according to claim 70, wherein the amount that said second network access device will restrict performance of the shared hosted application session is dependant on an ability of the second network access device to display information associated with the hosted application session.

73) A method for providing a shared hosted application session according to claim 68, wherein said determination of whether said second network access device is capable of participating in a shared hosted application session comprises determining whether said second network access device has adequate software installed to allow said second network access device to participate in a shared hosted application session.

74) A method for providing a shared hosted application session according to claim 68, wherein the step of communicating to said second network access device a capability verification request further comprises masking the capability verification request such that it is not readily discernible to said second participant.

75) A method for providing a shared hosted application session according to claim 68, wherein the step of communicating to said second network access device a capability verification request further comprises the step of encrypting the capability verification request prior to communicating the capability verification request to said  
5 second network access device.

76) A method for providing a shared hosted application session according to claim 68, wherein the step of communicating to said second network access device hosted application information further comprises masking the hosted application  
10 information such that it is not readily discernible to said second participant.

77) A method for providing a shared hosted application session according to claim 68, wherein the step of communicating to said second network access device hosted application information further comprises the step of encrypting the hosted  
15 application information prior to communicating the hosted application information to said second network access device.



78) A method for providing a shared hosted application session according to claim 68, wherein the step of communicating hosted application information to said second network access device further comprises the step of communicating the hosted application to the second network access device from the first network access device, the  
5 method further comprising the step of masking the hosted application information such that it is not readily discernible to a user of said first network access device.

79) A method for providing a shared hosted application session according to claim 68, wherein the step of communicating hosted application information to said  
10 second network access device further comprises the step of communicating the hosted application to the first network access device before the hosted application information is communicated to the second network access device, and wherein the step of communicating hosted application information to said first network access device further  
15 comprises the step of encrypting the hosted application information prior to communicating the hosted application information to said first network access device.

80) A method for providing a shared hosted application session according to claim 68, wherein said hosted application information for allowing said second network access device to share a hosted application session further comprises role information,  
20 said role information defining the authority of said second network access device to interact with a shared hosted application session.

81) A method for providing a shared hosted application session according to claim 80, wherein said role information is used to alternate control of a shared hosted application session between said first network access device and said second network  
5 access device.

82) A method for providing a shared hosted application session according to claim 80, wherein said second participant has an identity, and wherein said role information is dependant on said identity.  
10

83) A computer-readable medium tangibly embodying instructions which, when executed by a network access device, implement a process comprising the steps of:  
causing an instant messaging service to be instantiated on a first network access device, said first network access device having a first network connection to a network;  
15 causing the instantiated instant messaging service to establish a communications path with a remote network access device, said remote network access device having a second network connection to a the network;  
receiving at the first network access device a capability verification request;  
determining whether the first network access device meets capability  
20 requirements, said capability requirements identified in the capability verification request;

communicating to the remote network access device whether the first network access device meets capability requirements;  
when the first network access device meets capability requirements, receiving at the first network access device hosted application information; and

5           when said hosted application information indicates an available hosted application, attempting to establish a hosted application session with the available hosted application.

84)   A computer-readable medium tangibly embodying instructions according  
10   to claim 83, wherein said capability verification request comprises application server port information, and wherein said determination of whether the first network access device meets capability requirements comprises determining whether the first network access device is capable of communicating with a hosted application server via the application server port information.

15

85)   A computer-readable medium tangibly embodying instructions according  
to claim 84, wherein performance capabilities of said first network access device affect performance of a shared hosted application session, said affect being quantifiable as an amount, and wherein said determination of whether the first network access device meets  
20   capability requirements is dependant on the amount that said first network access device will restrict performance of a shared hosted application session.

86) A computer-readable medium tangibly embodying instructions according to claim 85, wherein the amount that said first network access device will restrict performance of a shared hosted application session is dependant on the bandwidth of the first network connection.

87) A computer-readable medium tangibly embodying instructions according to claim 85, said first network access device having a capability to display information associated with a hosted application session, wherein the amount that said first network access device will restrict performance of a shared hosted application session is dependant on said capability of the first network access device to display information associated with a hosted application session.

88) A computer-readable medium tangibly embodying instructions according to claim 83, wherein said determination of whether said first network access device is capable of participating in a shared hosted application training session comprises determining whether said first network access device has adequate software installed to allow said first network access device to share a hosted application session.

89) A computer-readable medium tangibly embodying instructions according to claim 83, said instructions implementing a process further comprising the step of decrypting hosted application information when received hosted application information is encrypted.

5

90) A computer-readable medium tangibly embodying instructions according to claim 83, said instructions implementing a process further comprising the step of receiving role information, said role information identifying the authority of the network access device to interact with a shared hosted application session.

10

91) A computer readable medium tangibly embodying instructions according to claim 83, said instructions implementing a process further comprising the step of controlling interaction between a computer executing the process and a shared hosted application.

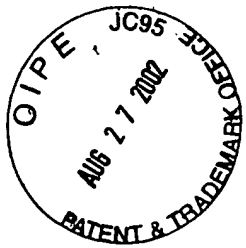
15

92) A computer readable medium tangibly embodying instructions according to claim 91, wherein the step of controlling interaction is dependant on an identity associated with a user of the computer executing the process.

93) A computer readable medium tangibly embodying instructions according to claim 91, wherein said hosted application information comprises role information, and the step of controlling interaction is dependant on said role information.

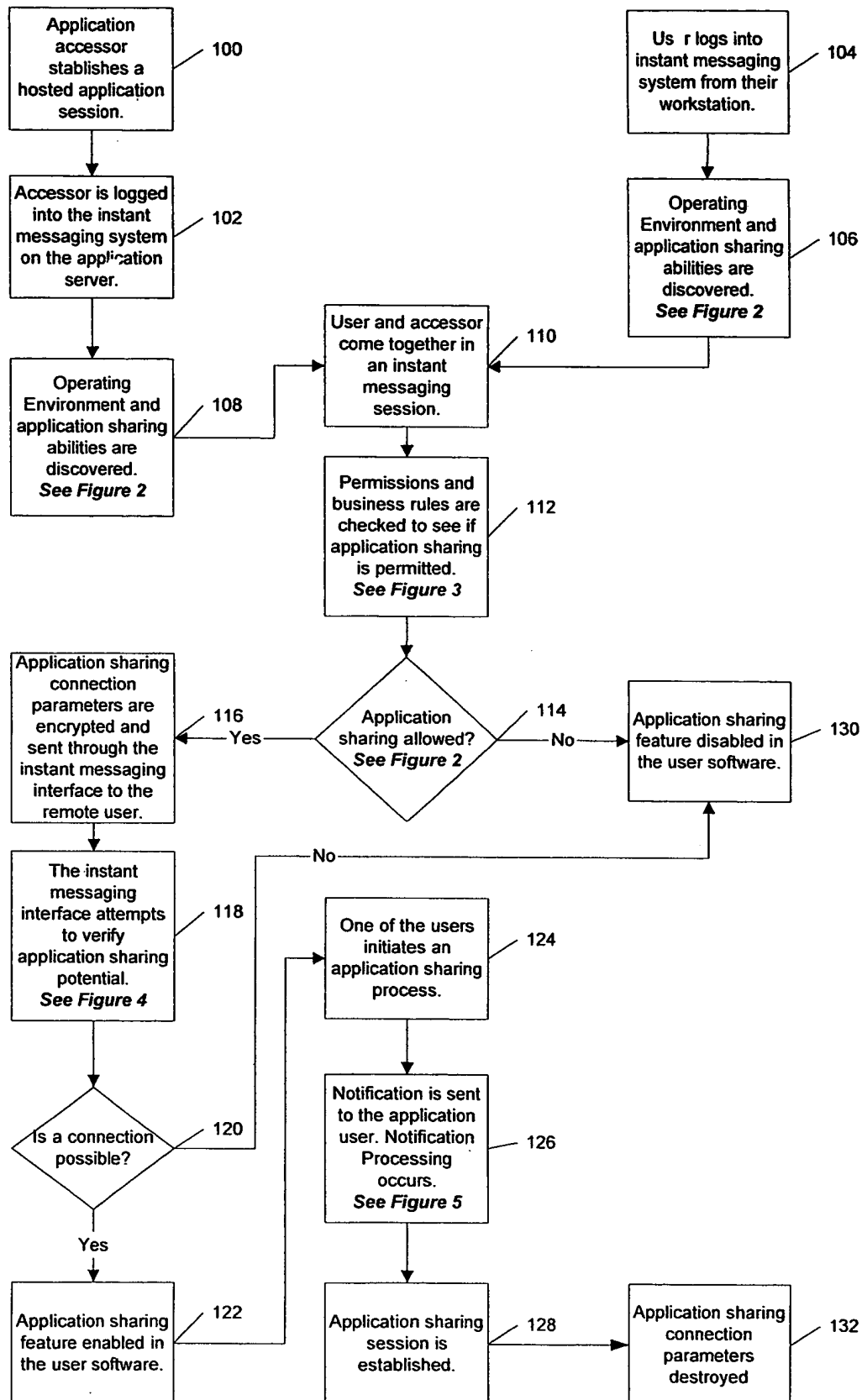
### **Abstract**

5           The present invention is a system and method for using an instant messaging environment to facilitate the establishment of hosted application sharing sessions between a hosted application user and one or more other users in an instant messaging environment. The present invention utilizes a real-time instant messaging system to communicate necessary information between two messaging clients, allowing conditional  
10 limitations to be applied to the application sharing process, as well as providing a simplified method to allow shared application users to collaborate in a hosted application session.



# Figure 1

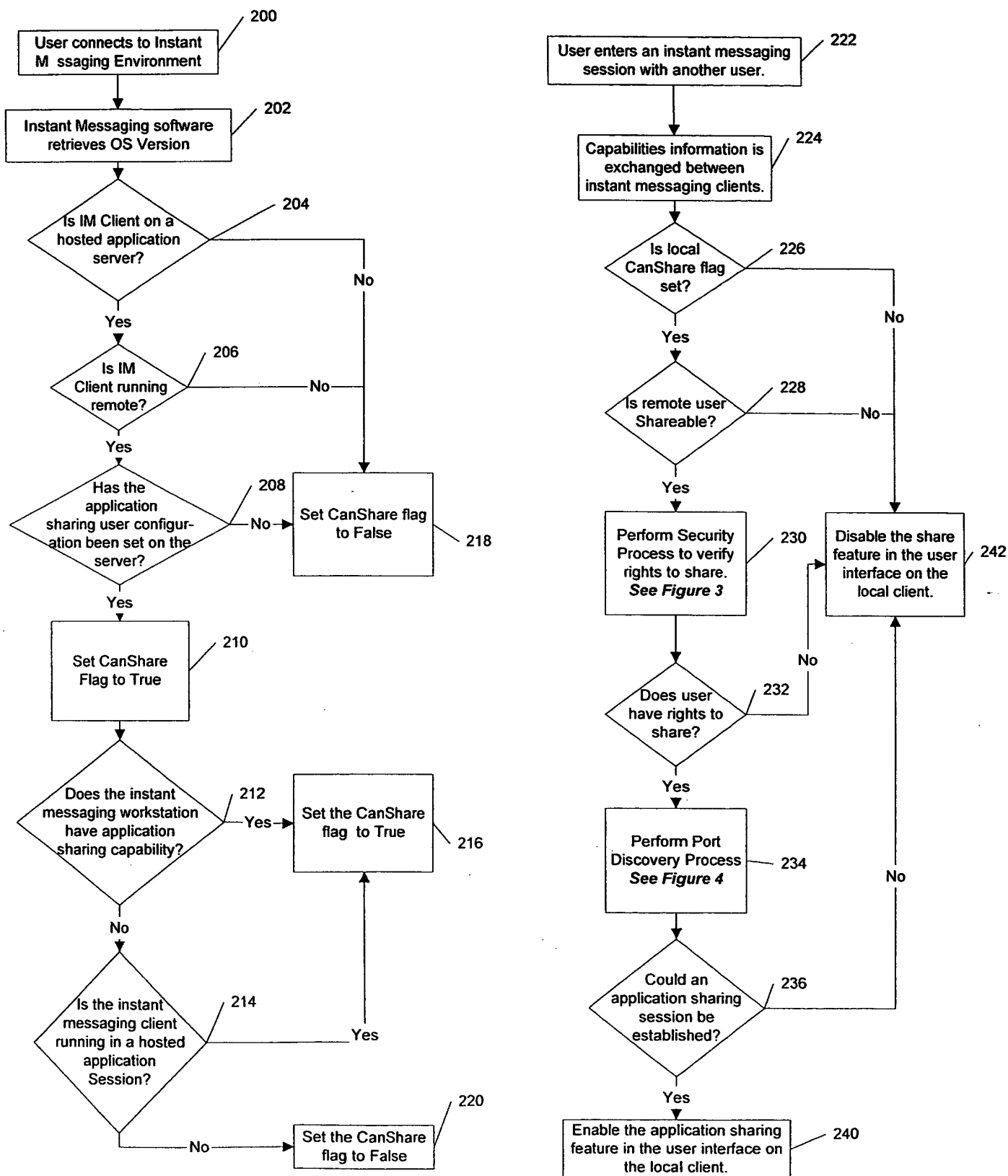
Example of a User-to-User Collaboration Embodiment





## Figure 2

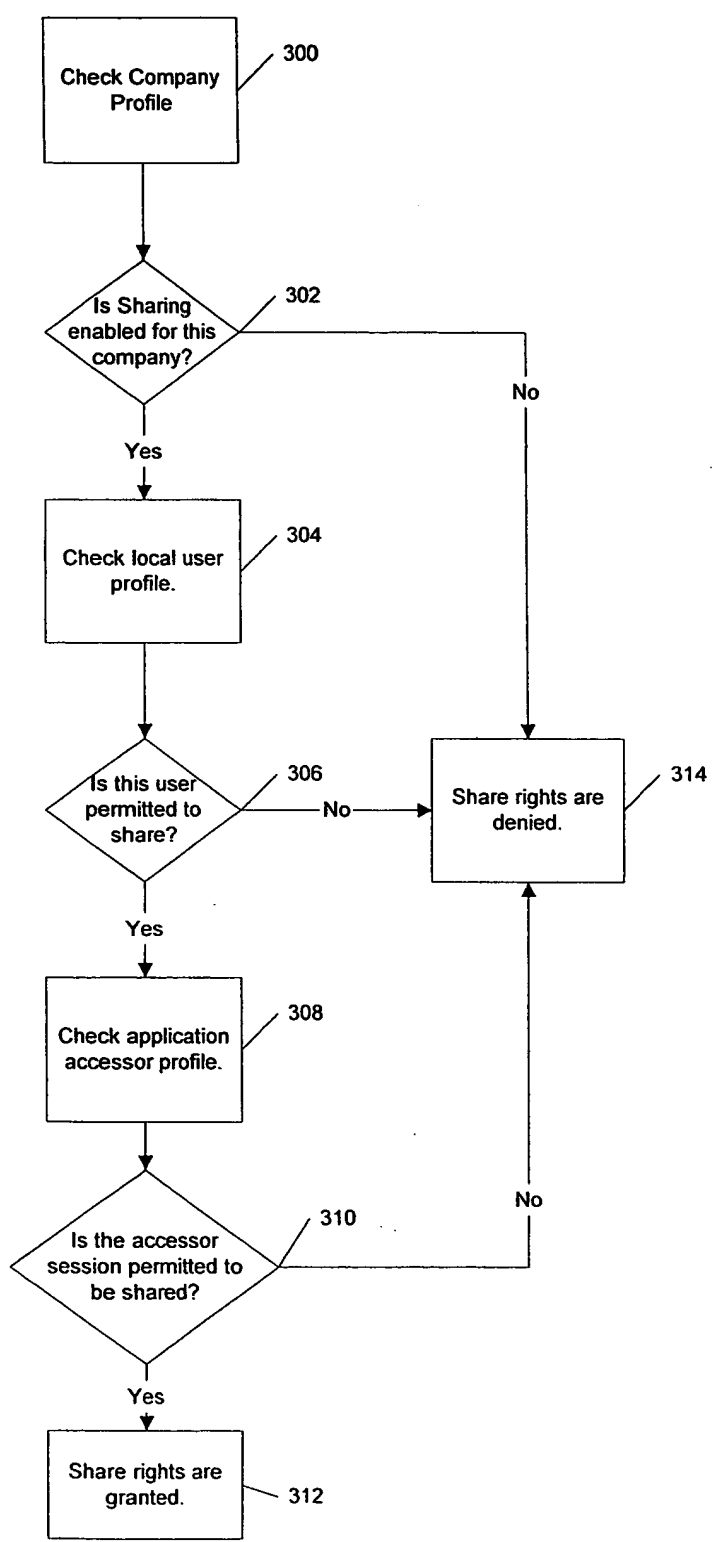
Capability Discovery and Exchange Process





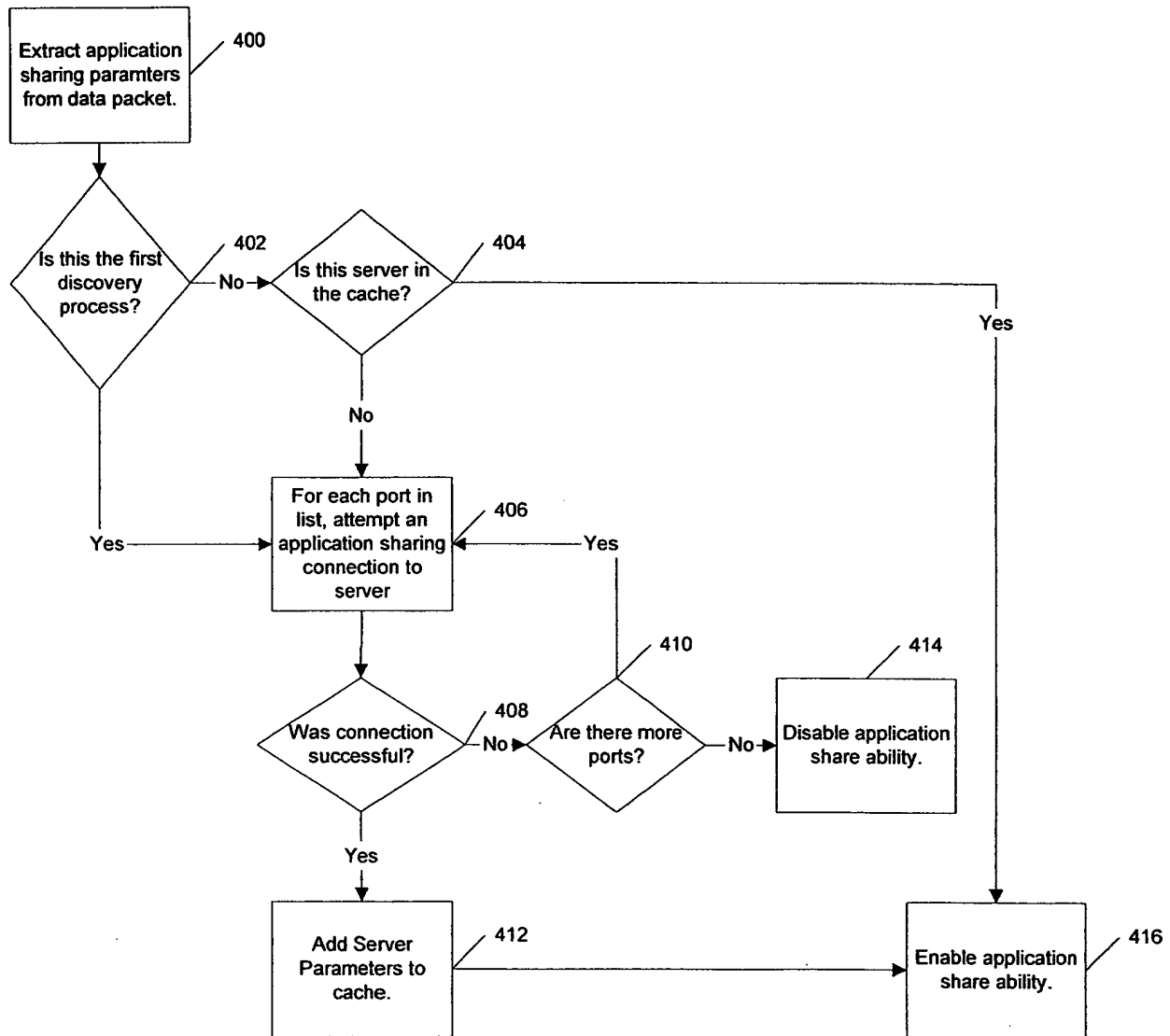
# Figure 3

Security Processing for Application Share Ability





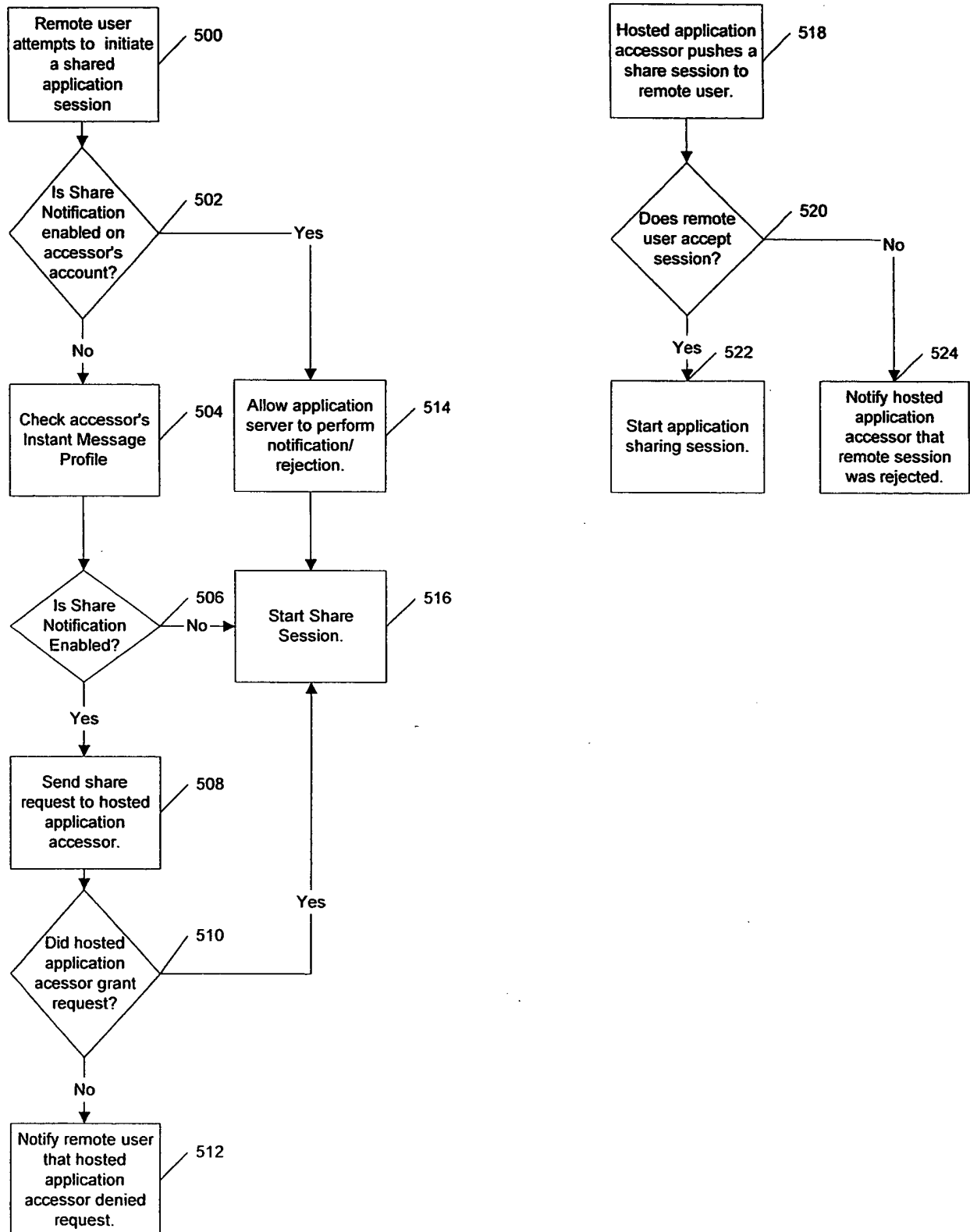
**Figure 4**  
Port Discovery Process





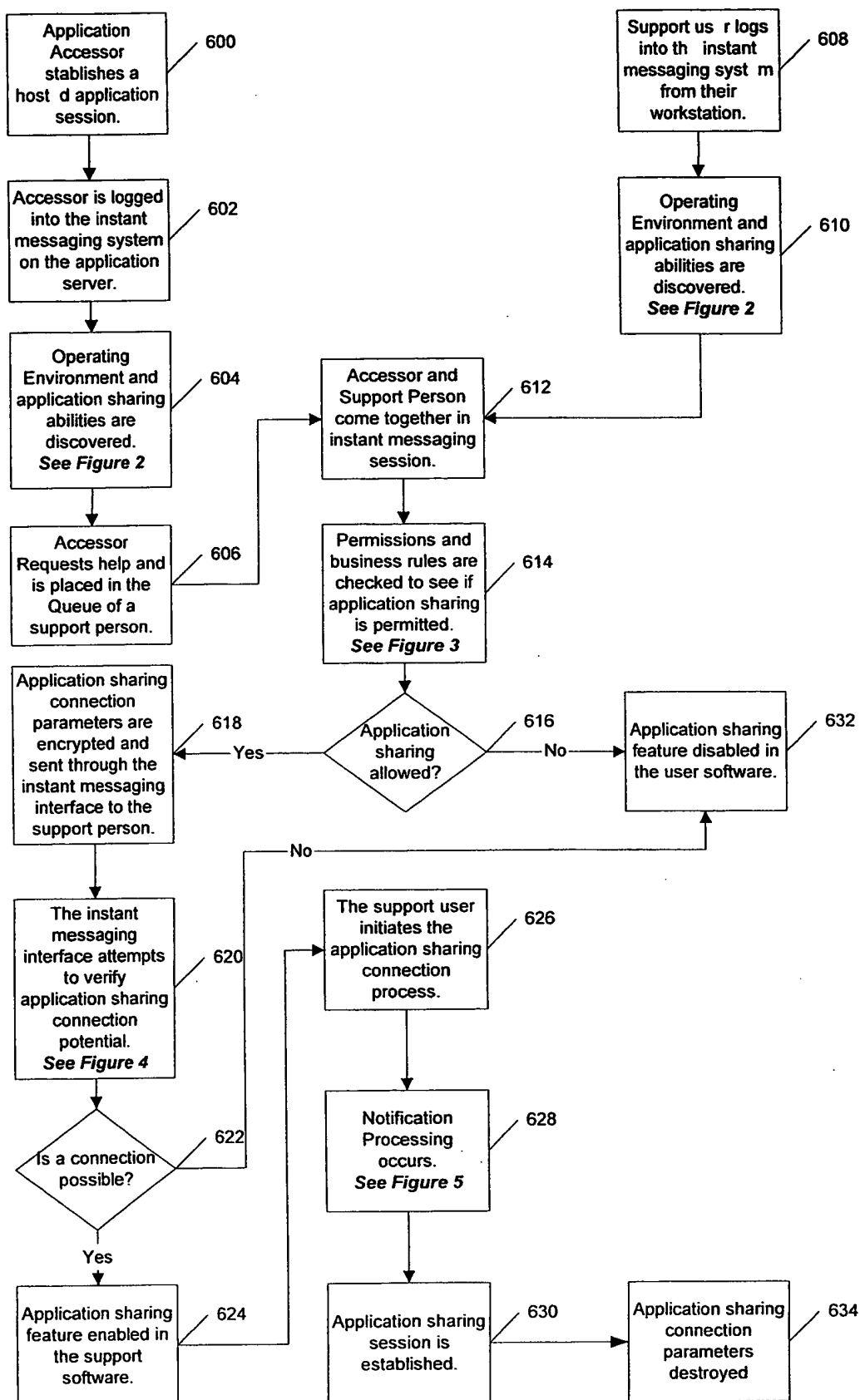
# Figure 5

Notification Processing for Application Share Request



## Figur 6

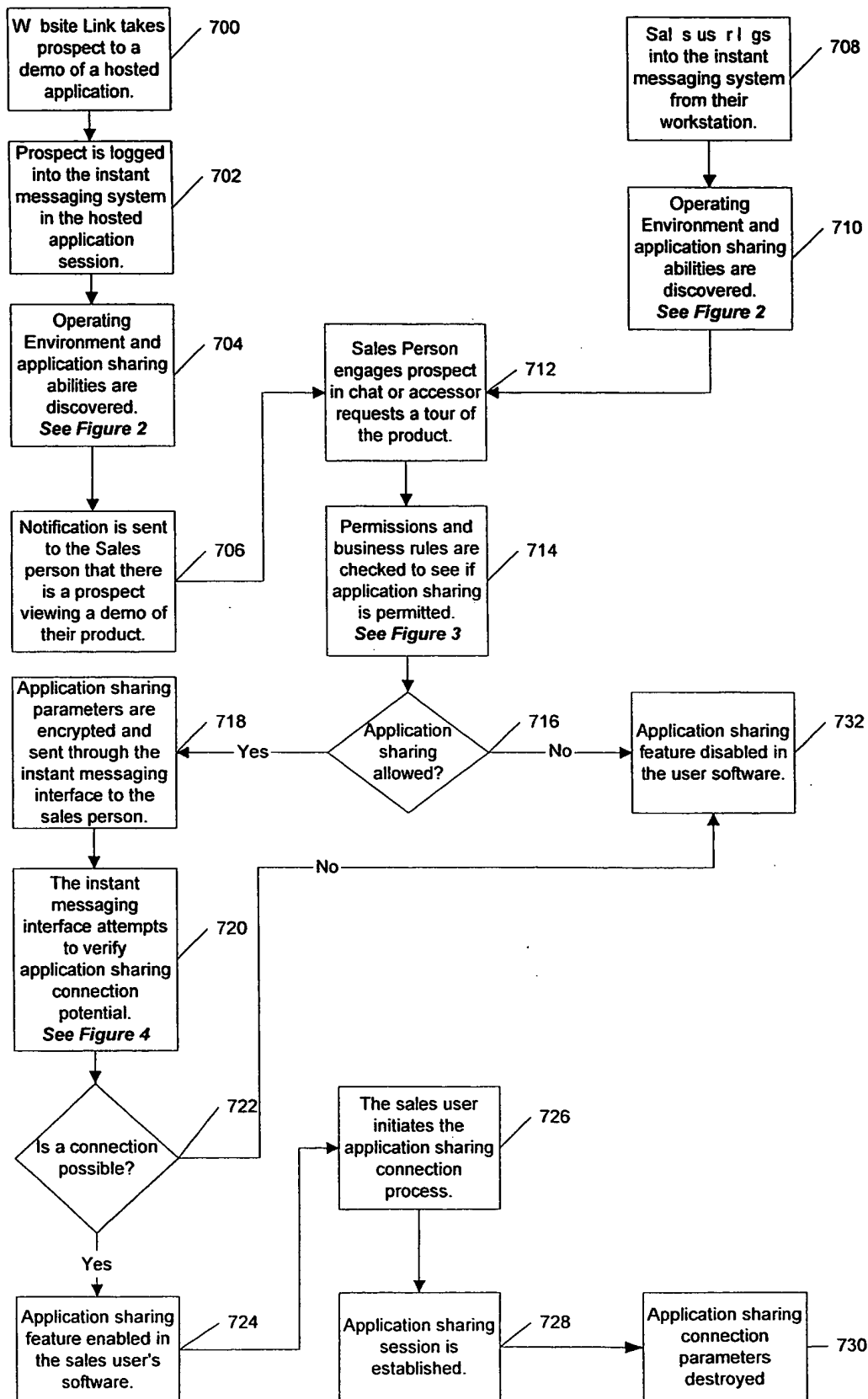
Examl of a Supp rt r H lp Desk Collab rativ Emb diment.





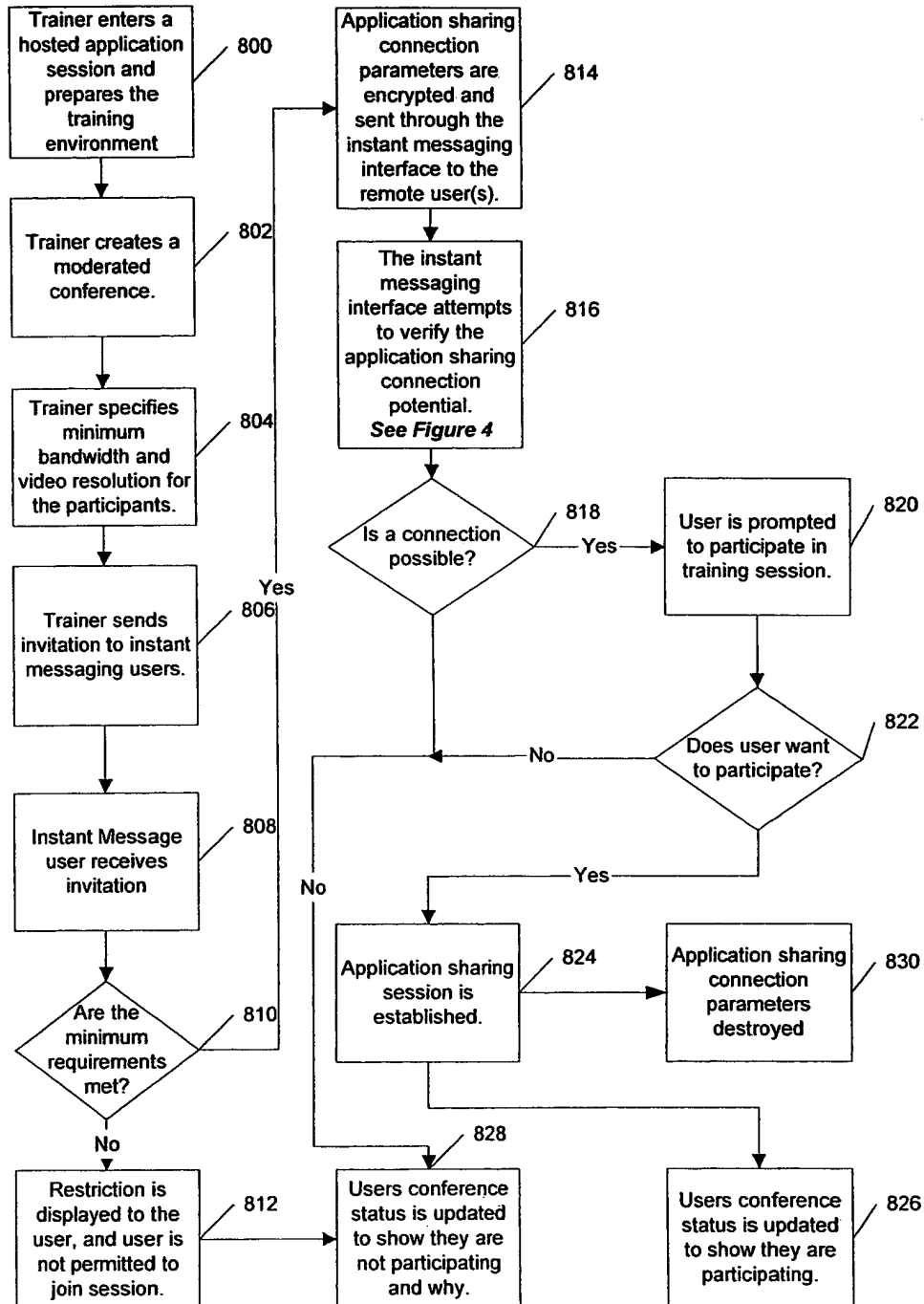
# Figure 7

Example of a Sales Process Embodiment.



# Figure 8

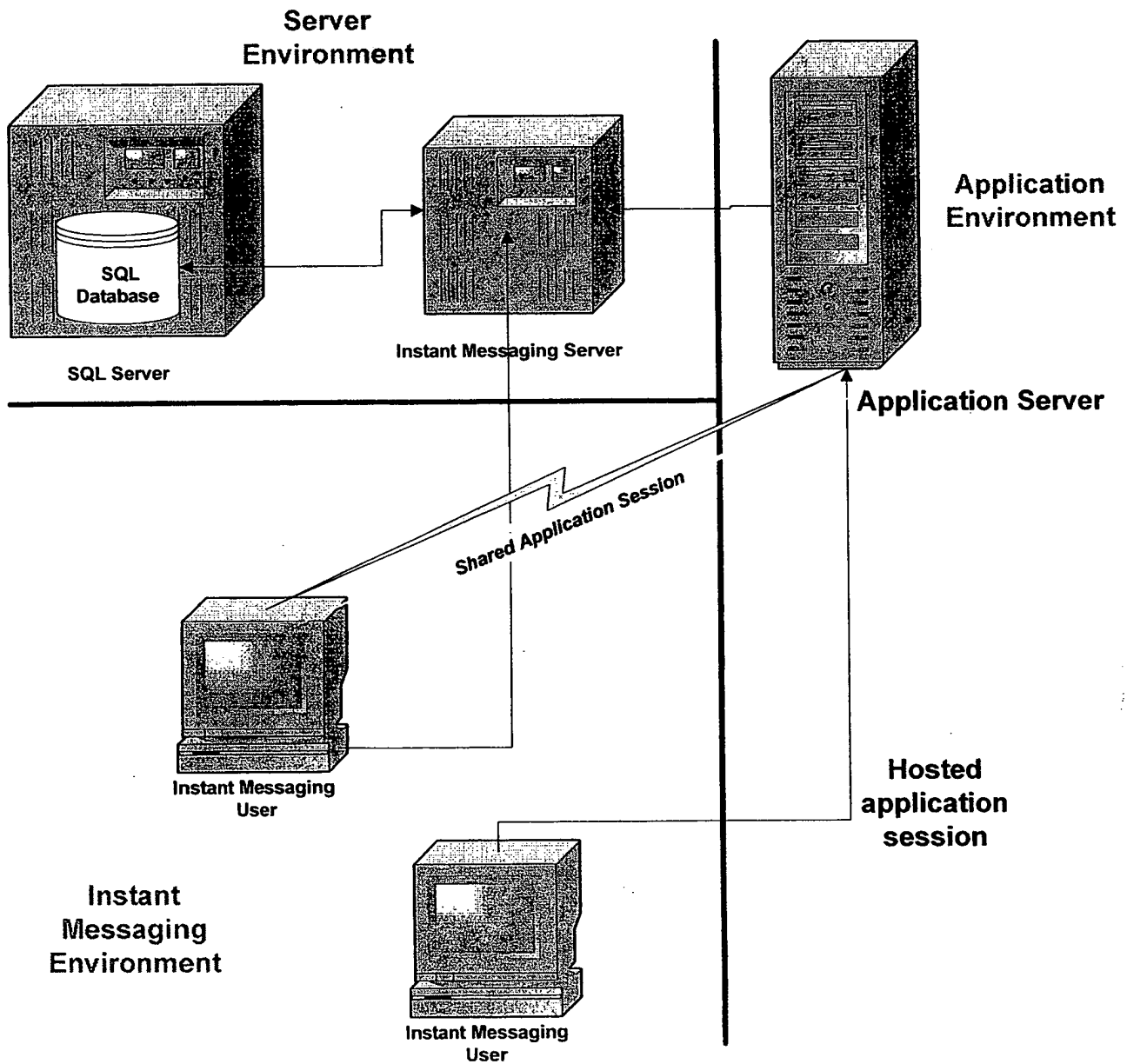
Example of a Training Session Embodiment.





**Figure 9**

System Component Overview







IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of Turner et al.	:	Attorney Docket No.:
	:	01-40169-US
Serial No.:	:	
Conf. No.:	:	
	:	Group Art Unit:
Filed:	:	Unknown
	:	
For:	:	Examiner:
SYSTEM AND METHOD FOR	:	Unknown
USING AN INSTANT	:	
MESSAGING ENVIRONMENT	:	
TO ESTABLISH A HOSTED	:	
APPLICATION SHARING	:	
SESSION	:	

**DECLARATION OF JONATHAN M. DARCY**

I, Jonathan M. Darcy of Reed Smith LLP, an attorney of record for the above-identified patent application, make this Declaration in support of Applicant's Petition To Withdraw Notice of Omitted Items In a Non Provisional Application. Except where noted otherwise, all statements made in this Declaration are based on my personal knowledge.

1. I am an attorney of record for U.S. Patent Application serial no. 10/015,077 (the "Application") and attended to filing the Application on October 26, 2001 as part of my duties as an attorney with Reed Smith LLP (the "Firm").

2. Upon information and belief, it is the standard practice for our Firm to file patent applications utilizing the Express Mail service provided by the United States Postal Service, and in conformance with 37 C.F.R. §1.10.

3. It is, and has been since prior to October 26, 2001, my standard practice to file patent applications utilizing the Express Mail service provided by the United States Postal Service, and in conformance with 37 C.F.R. §1.10.

4. Upon information and belief, it is the standard practice for our Firm that patent applications being filed with the United States Patent and Trademark Office be reviewed by a registered patent practitioner immediately before the application is placed into an Express Mail envelope. This review includes a page by page verification that the complete application, including all Figures, is present immediately before the application is placed into the Express Mail envelope for transmission.

5. It is my standard practice, and has been since prior to October 26, 2001, for patent applications I am filing, to personally review the application by, among other things, personally verifying that each sequentially numbered page is present, that each page of claims is present, and that each of the Figures is present prior to signing the transmittal letter and application cover sheet.

6. I signed the transmittal letter and application cover sheet for the Application.

7. It is my standard practice, and has been since prior to October 26, 2001, that after I sign the application cover sheet and transmittal letter, to then request that the completed application be photocopied. It is my standard practice, and has been since prior to October 26, 2001, for patent applications I am filing, to again personally review the application after photocopying by, among other things, personally verifying that each sequentially numbered page is present, that each page of claims is present, and that each of the Figures is present in both the original and at least one photocopy. It is my standard practice, and has been since prior to October 26, 2001, that once I complete this second review, the original application and supporting documents are placed into the Express Mail envelope and sealed in my presence. The sealed Express Mail envelope is then deposited with the local Post Office in accordance with the procedures of our Firm.

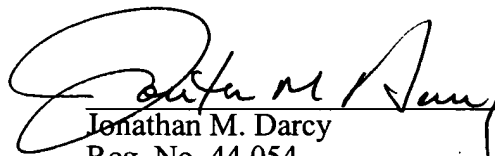
8. I do not recall, since joining Reed Smith, even a single instance of when I did not follow my standard practice for filing patent applications.

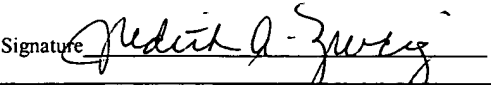
9. Upon information and belief, the Application was transmitted via Express Mail in conformance with 37 C.F.R. § 1.10 and with the Firm's established and regularly employed procedures for filing documents by Express Mail. Transmission and receipt of the Express Mail envelope containing the Application are not contested to my knowledge.

10. It is my belief, based on the standard practices of our Firm, as well as my own standard practice and lack of recollection of even a single instance of failing to follow my standard practice for filing patent applications, that the complete Application, including pages 19-23, were transmitted to the United States Patent and Trademark Office on October 26, 2002.

I, Jonathan M. Darcy, declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the Application.

Dated: 8/27/02

  
Jonathan M. Darcy  
Reg. No. 44,054

EXPRESS MAIL CERTIFICATE (37 CFR 1.10)	
Express Mail Label No. <u>EL166821225 US</u>	Date of Deposit <u>Aug 27, 2002</u>
I hereby certify that this paper, and the papers and/or fees referred to herein as transmitted, submitted or enclosed, are being deposited with the U.S. Postal Service "Express Mail Post Office to Addressee" service under 37 CFR §1.10 on the date indicated above and is addressed to Assistant Commissioner for Patents, Box, DAC, Washington, D.C. 20231.	
Name <u>JUDITH A. ZWEIG</u>	Signature 



BEST AVAILABLE COPY

Pat./Serial No. NOT Yet Assigned

Title System and Method for Using An Instant Messaging Environment To Establish A Hosted Application Sharing Session

Appl. / Patentee TURNER et al.

Atty. Docket # 01-40169-US  
882397.2000.1038

The Patent and Trademark Office acknowledges, and has stamped hereon, the date of the receipt of the items listed below:

1. Cert. of Mailing:  
1st Class Date \_\_\_\_\_

Express Mail Date 10/26/01

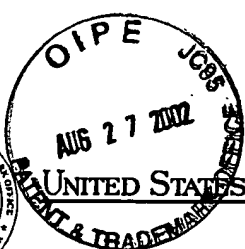
Label No. EL166824093US

1. Utility Patent  
Application Transmitted

2. Cover letter

3. Patent Application  
67 sheets; 9 sheets  
drawings

4. Declaration and  
Power of Attorney  
(unsigned)



## UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS  
UNITED STATES PATENT AND TRADEMARK OFFICE  
WASHINGTON, D.C. 20231  
www.uspto.gov

APPLICATION NUMBER	FILING DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	DRAWINGS	TOT CLAIMS	IND CLAIMS
10/015,077	10/26/2001	2152	0.00	01-40169- US	9	93	7

CONFIRMATION NO. 9530

07066  
REED SMITH LLP  
2500 ONE LIBERTY PLACE  
1650 MARKET STREET  
PHILADELPHIA, PA 19103

## FILING RECEIPT



\*OC00000007371461\*

Date Mailed: 01/28/2002

Receipt is acknowledged of this nonprovisional Patent Application. It will be considered in its order and you will be notified as to the results of the examination. Be sure to provide the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION when inquiring about this application. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please write to the Office of Initial Patent Examination's Customer Service Center. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections (if appropriate).

## Applicant(s)

Tod Turner, Lake Forest Park, WA;  
Bruce Bequette, Lynwood, WA;  
Wade Lance, Kirkland, WA;  
Bryan Schremp, Bothell, WA;

## Domestic Priority data as claimed by applicant

THIS APPLN CLAIMS BENEFIT OF 60/242,395 10/20/2000

## Foreign Applications

If Required, Foreign Filing License Granted 01/24/2002

Projected Publication Date: To Be Determined - pending completion of Missing Parts

Non-Publication Request: No

Early Publication Request: No

## Title

System and method for using an instant messaging environment to establish a hosted application sharing session

DOCKETED

Lms 2/1/02

Preliminary Class

709

---

**LICENSE FOR FOREIGN FILING UNDER  
Title 35, United States Code, Section 184  
Title 37, Code of Federal Regulations, 5.11 & 5.15**

**GRANTED**

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Office of Export Administration, Department of Commerce (15 CFR 370.10 (j)); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

**NOT GRANTED**

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).